



European
Commission

EU Privacy seals project

Inventory and analysis of privacy
certification schemes

Final Report Study Deliverable 1.4

Authors

Rowena Rodrigues,
David Barnard-Wills,
David Wright,
Paul De Hert,
Vagelis Papakonstantinou,

Editors

Laurent Beslay, EC JRC-IPSC
Nicolas Dubois, EC DG JUST

2013

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

<http://ipsc.jrc.ec.europa.eu/>
<http://www.jrc.ec.europa.eu/>

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/>.

JRC 85092

EUR 26190 EN

ISBN 978-92-79-33275-3

ISSN 1831-9424

doi: 10.2788/29861

Luxembourg: Publications Office of the European Union, 2013

© European Union, 2013

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 DGs¹, the LIBE committee secretariat of the European Parliament, ENISA. This report constitutes the first deliverable of the study.

The authors of this report are:

- Rowena Rodrigues, Associate Partner, Trilateral
- David Barnard-Wills, Associate Partner, Trilateral
- David Wright, Managing Partner, Trilateral
- Paul De Hert, Vrije Universiteit Brussel
- Vagelis Papakonstantinou, Vrije Universiteit Brussel

In addition, the report has benefited from comments and suggestions made by:

- Luca Remotti, Intrasoft International S.A.
- as well as 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 G07 - 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

1	Introduction	10
2	Objectives	11
3	Methodology	11
4	The importance of privacy seals	12
4.1	Guarantee privacy	13
4.2	Build and enhance consumer trust and confidence	14
4.3	Support business, trade and economic growth.....	15
4.4	Foster adherence to privacy, data protection standards	16
4.5	Generate privacy accountability	17
4.6	Promote overall awareness of privacy and data protection	17
4.7	Easy and quick representation of privacy and data protection commitments.....	18
4.8	Flexible privacy and data protection mechanism.....	18
4.9	Dispute solving mechanism	18
5	Criteria for evaluation and comparison of privacy seals	18
5.1	General criteria.....	18
5.2	Criteria based on the GDPR requirements.....	19
5.3	Collated criteria.....	28
6	Identification and analysis of privacy seal schemes	28
6.1	List of privacy seal schemes	28
6.2	The research scope, limitations and problems	29
6.2.1	<i>Lack of availability and easy accessibility to information.....</i>	<i>29</i>
6.2.2	<i>Difficulty finding the specific criteria or requirements for award of seals.....</i>	<i>30</i>
6.2.3	<i>Lack of response to information requests</i>	<i>30</i>
6.2.4	<i>Necessity of relying on second and third party information</i>	<i>30</i>
6.2.5	<i>Language barriers.....</i>	<i>31</i>
6.2.6	<i>Non-availability of certain schemes</i>	<i>31</i>
6.2.7	<i>Name changes</i>	<i>31</i>
6.2.8	<i>Lack of discussion of the GDPR.....</i>	<i>31</i>
6.3	Analysis of privacy seal schemes against general criteria	32
6.3.1	<i>Nature.....</i>	<i>32</i>
6.3.2	<i>Country.....</i>	<i>33</i>
6.3.3	<i>Inception.....</i>	<i>34</i>
6.3.4	<i>Issuing organisation and issuer type.....</i>	<i>36</i>
6.3.5	<i>Target of scheme and entities that can be certified.....</i>	<i>36</i>
6.3.6	<i>Number of certified entities</i>	<i>38</i>
6.3.7	<i>Validity and renewals.....</i>	<i>39</i>
6.3.8	<i>Types of beneficiaries.....</i>	<i>40</i>
6.3.9	<i>Objectives of the scheme</i>	<i>41</i>
6.3.10	<i>Descriptive summary of the schemes and unique selling points</i>	<i>42</i>
6.3.11	<i>Privacy and data protection elements of the schemes</i>	<i>42</i>
6.3.12	<i>Guarantees offered to data subjects.....</i>	<i>43</i>

6.3.13	<i>Duration, scope and steps in the certification process</i>	44
6.3.14	<i>Coverage of international transfers</i>	45
6.3.15	<i>Costs</i>	45
6.3.16	<i>Revocation</i>	46
6.3.17	<i>Recognition</i>	47
6.3.18	<i>Accredited experts, evaluation bodies and certified experts</i>	49
6.3.19	<i>Regulatory and compliance standards</i>	49
6.3.20	<i>Frequency and means of updates to schemes</i>	51
6.3.21	<i>Additional elements</i>	52
6.3.22	<i>Complaints mechanisms</i>	52
6.3.23	<i>Criticisms</i>	52
6.3.24	<i>Links and references to schemes</i>	54
6.3.25	<i>Logos</i>	54
6.3.26	<i>Websites</i>	56
6.4	<i>Analysis of privacy seal schemes against GDPR criteria</i>	56
6.4.1	<i>Principles</i>	57
6.4.2	<i>Rights of the data subject</i>	58
6.4.3	<i>Controller and processor obligations</i>	60
6.4.4	<i>Transfer of personal data to third countries or international organisations</i>	61
7	Main convergences and differences	61
7.1	Seal accessibility models	61
7.2	Scheme objectives	81
7.3	EU schemes and non-EU based schemes	81
7.4	Compliance and regulatory standards	85
7.5	Rights of data subjects	86
7.6	Complaints redress	86
7.7	Shared problems	89
7.8	GDPR requirements	89
8	Beneficiaries of privacy seals	91
8.1	Beneficiaries and benefits	91
8.1.1	<i>Government</i>	91
8.1.1.1	Policy makers	91
8.1.1.2	Regulators	92
8.1.1.3	Other public bodies	93
8.1.2	<i>Industry</i>	93
8.1.2.1	Issuers of privacy seals	93
8.1.2.2	Privacy seal buyers – large enterprises	94
8.1.2.3	Privacy seal buyers – small and medium enterprises	95
8.1.2.4	Third parties (e.g. independent evaluators, auditors)	96
8.1.2.5	Industry associations	96
8.1.3	<i>Privacy/data protection organisations</i>	97
8.1.4	<i>Consumers</i>	97
8.1.5	<i>Individuals</i>	98
8.1.6	<i>Society</i>	98
8.2	Impacts on beneficiaries	100
9	Conclusions	102

10	References	106
11	Annex I – Individual privacy seal profiles	111
11.1	BBB accredited business seal	113
11.2	buySAFE Guaranteed shopping.....	118
11.3	Cloud Security Alliance	126
11.4	CNIL Label	132
11.5	Comodo Secure	138
11.6	Confianza Online	143
11.7	Danish e-mark.....	148
11.8	ePrivacy Seal.....	152
11.9	ESRB Privacy Online Certification	156
11.10	Euro-Label	165
11.11	EuroPriSe	170
11.12	Gigya's SocialPrivacy™ Certification	176
11.13	Market Research Society (MRS) Fair Data Mark.....	182
11.14	McAfee Secure.....	189
11.15	PrivacyMark System	195
11.16	Privo Privacy certified	202
11.17	Seriedad Online.....	209
11.18	Smart Grid Privacy Seal.....	214
11.19	Transaction Guard Privacy Policy Verified Seal	221
11.20	TRUSTe	225
11.21	Trusted Shops.....	232
11.22	Trustify-Me Privacy Certification Seal.....	239
11.23	TÜV Trusted Site Privacy Certification Mark.....	243
11.24	Verified by Visa.....	249
11.25	WebTrust Privacy Seal	256
12	Annex II – “Fingerprints” of individual seal schemes	264
12.1	BBB Accredited Business Seal	264
12.2	BuySafe Guaranteed Shopping	265
12.3	Cloud Security Alliance	266
12.4	CNIL label	267
12.5	Comodo Secure	268
12.6	Confianza Online	269
12.7	Danish e-mark.....	270
12.8	ePrivacyseal	271
12.9	ESRB Privacy Online Certification	272
12.10	Euro-label.....	273
12.11	EuroPriSe (European Privacy Seal)	274
12.12	Gigya's SocialPrivacy™ Certification	275
12.13	Market Research Society (MRS) Fair Data	276

12.14 McAfee Secure.....	277
12.15 PrivacyMark System.....	278
12.16 Privo Privacy certified	279
12.17 Seriedad Online.....	280
12.18 Smart Grid Privacy Seal.....	281
12.19 Transaction Guard Privacy Policy Verified Seal	282
12.20 TRUSTe	283
12.21 Trusted Shops.....	284
12.22 Trustify-Me Privacy Certification Seal.....	285
12.23 TÜViT Trusted Site privacy	286
12.24 Verified by Visa.....	287
12.25 WebTrust.....	288

List of tables

Table 1 Organisational representation.....	10
Table 2 General criteria for evaluation of privacy seal schemes	19
Table 3 GDPR requirements-based criteria for evaluation of privacy seal schemes	28
Table 4 Nature-based classification of schemes	32
Table 5 Geographical location of scheme operators	33
Table 6 Organisation-based categorisation of schemes	36
Table 7 Targets and schemes	37
Table 8 Number of certified entities	38
Table 9 Number of certified entities by organisation type.....	39
Table 10 Number of certified entities by nature of seal.....	39
Table 11 Grounds of revocation.....	46
Table 12 Regulatory and compliance standards.....	51
Table 13 Criticisms	53
Table 14 Model-based classification of schemes	63
Table 15 Categories for key variables.....	76
Table 16 CSA scheme characteristics	77
Table 17 Conianza Online characteristics.....	78
Table 18 Density map of the shared characteristics of the analysed schemes	79
Table 19 Characteristics of the US-based seals	83
Table 20 Characteristics of the Europe-based schemes	84
Table 21 Standards and schemes.....	85
Table 22 Complaints mechanisms and nature of the schemes	87
Table 23 Complaints mechanisms and privacy and data protection elements.....	88
Table 24 Complaints mechanisms and nature of certifying authority	88
Table 25 Beneficiaries-benefits summary.....	99
Table 26 Beneficiaries and impact	100
Table 27 Collated scheme assessment table.....	112

List of figures

Figure 1 Inception timeline	34
Figure 2 Scheme logos	54
Figure 3 Legends for the seal models.....	63
Figure 4 Classic or minimal seal model	64
Figure 5 The linked seal model	65
Figure 6 A hosted seal model	66
Figure 7 External standards seal model.....	67
Figure 8 Delegated certification model	68
Figure 9 Federated seal model	69
Figure 10 Security scan model	70
Figure 11 Insurance seal model.....	71
Figure 12 Self-assessment register model	72
Figure 13 Investigative registry.....	73
Figure 14 3-D Secure model	74
Figure 15 Combination of seal models	75

1 INTRODUCTION

Privacy seals schemes are voluntary privacy measures adopted as a self-regulatory initiative to promote consumer trust and confidence in e-commerce.² They enable organisations to demonstrate respect for privacy and develop a trustworthy image. Their importance has been recognised at the international, European and national level. However, meaningful certification depends upon the scope of the certification process and the roles of the actors involved.

The subject of contract 258065 is a Study on EU privacy seals. The overall objectives of this study are:

- to identify and analyse the scientific and organisational success factors for which it will be opportune and feasible to launch a European-wide privacy certification scheme,
- to assess the scope and rules of such a scheme, the roles of the various public and private stakeholders in its development, and
- to assess the impact on existing legislation and the interaction with existing mechanisms guaranteeing privacy (such as the ones foreseen by Directive 95/46/CE, the proposed General Data Protection Regulation (GDPR) of 25 of January 2012³ and existing national privacy seals).

This report presents the results of *Task 1 of the Privacy Seals Study – Inventory and analysis of existing privacy certification schemes*. The task is led by Trilateral Research & Consulting. Vrije Universiteit Brussel has contributed as outlined specifically in the document.

The organisational representation for the purposes of this report is as follows:

	Lead contact	Contributors
Trilateral Research & Consulting	David Wright	Rowena Rodrigues David Barnard-Wills
Vrije Universiteit Brussel	Paul de Hert	Vagelis Papakonstantinou

Table 1 Organisational representation

The Advisory Board members, Kirsten Bock (ULD, Office of the Data Protection and Freedom of Information Commissioner of Schleswig-Holstein), Kostas Rossoglou (Senior Legal Officer, BEUC), and Douwe Korff (Professor of International Law, London Metropolitan University) along with consortium partner Luca A. Remotti (Intrasoft International SA) reviewed this deliverable and provided helpful comments.

² European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions, *A European Consumer Agenda - Boosting confidence and growth* SWD (2012) 132 final Brussels, 22.5.2012. This document recognises the need to improve consumer confidence in cross-border shopping online by taking appropriate policy action. According to it, “empowered and confident consumers can drive forward the European economy”.

³ 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

2 OBJECTIVES

The objective of this report is to comprehensively inventory and analyse privacy and related certification schemes in the European Union and, where relevant, at the international level.⁴ The report will provide insights into the importance of privacy seal schemes and present information on the operational aspects of these schemes. The report will also help understand the privacy and data protection elements of the analysed schemes and provide an initial analysis of their shortcomings. The report specifically aims to understand whether (if at all) the analysed schemes address the requirements proposed under the GDPR. It will highlight the main convergences and differences between the schemes, who benefits from such schemes and what the impact of such schemes is.

3 METHODOLOGY

The study team conducted a literature review (academic, policy and technical) to collate and finalise criteria (based on EU Privacy Seals Tender Specifications⁵ and the proposal) for evaluating the different privacy certification schemes. The criteria have two levels: general and specific in relation to the General Data Protection Regulation.

Next, the study team listed various privacy and related certification schemes, adopting a broad approach based on the tender specifications, and analysed them against set criteria. The listed schemes are not only privacy and data protection specific schemes; some are general trust mark schemes covering a heterogeneous range of privacy and data protection related issues. The team collected information for all of the identified privacy and privacy-related schemes through desktop research and where necessary through correspondence with the relevant privacy seal issuers and other stakeholders such as policy-makers and regulators (data protection authorities).

Using pattern recognition and comparative methodologies, the study team conducted an analysis of privacy seals. Visual data help illustrate the relationship between privacy seals and each of the parameters and demonstrate their relationship with one another. This provided valuable data and highlights the nature, convergences and distinctions between the different, existing privacy seals.

The study team considered key functional aspects, comparing the approaches to functional, legal, technical privacy assessment of the different seals and producing a synthesis of the possible models, sets of features and functions of a privacy seal. The report draws some conclusions on the relationship between the objectives and forms of privacy certification schemes and their operational factors.

The study team also carried out an analysis of beneficiaries as outlined in section 8.

⁴ Note that the list of schemes analysed in this report was per Tender Specifications. Some of the schemes specified for analysis were not strictly privacy or data protection focussed.

⁵European Commission Joint Research Centre, *Study on EU Privacy Seals*, Invitation to Tender No. 2012/S 179-293767 of 18 Sept 2012.

4 THE IMPORTANCE OF PRIVACY SEALS

Privacy seals are an important privacy protection mechanism. Various levels of government, industry and community have recognised their role and significance.⁶ From the regulator's perspective, privacy seal schemes may help reduce the regulatory and enforcement burden – meaning less need for regulation (greater regulation entails greater legal compliance and enforcement costs) and greater flexibility. Privacy seal schemes have the capacity to foster a respect for legal and industry standards that lessens the need to increase legal regulation which comes with its own costs. However, a key element of an effective privacy seal scheme is effective privacy compliance and enforcement, and privacy seal schemes in their current form are not an alternative to data protection and privacy regulation. From the industry's perspective, privacy seals promote certified entities, build consumer trust and confidence and bring market advantages. Privacy certification helps organisations demonstrate their privacy values and commitments, including a commitment to uphold the rights of data subjects, including their right to access and, if necessary, correct their personal data. From the community perspective, privacy seals help consumers, users and the general public make quick judgements about an organisation's privacy and data protection policies and practices.

Article 39 of the proposed General Data Protection Regulation calls for “the establishment of data protection certification mechanisms and of data protection seals and marks”, as a means of enabling data subjects to “assess the level of data protection provided by controllers and processors”.⁷

Several other EC documents draw attention to the importance of and need for privacy seals. The European Commission's 2007 Communication on privacy-enhancing technologies (PETs) speaks of privacy seals as means of facilitating consumers' informed choice – and suggests that their purpose is to “ensure consumers can easily identify a certain product as ensuring or enhancing data protection rules in the processing of data, in particular by incorporating appropriate PETs”.⁸ The Kantor *Final Report on New Challenges to Data Protection* prepared for the European Commission's Directorate General of Justice, Freedom and Security (EC DG JFS, as it was then named) discusses privacy seals and maintains that they are a low-tech solution to protect data.⁹

The Council of the European Union “supports the idea of introducing privacy seals (EU certification schemes) and self-regulatory initiatives; both initiatives would involve close

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; Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, 2006, p. 122; Miyazaki, A., and S Krishnamurthy, “Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions”, *Journal of Consumer Affairs*, Vol. 36, No. 1, 2002, p. 28.

⁷ European Commission, COM (2012) 11 final, op. cit., 25 Jan 2012.

⁸ European Commission, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM/2007/0228 final, Brussels, 2 May 2007. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF>

⁹ LRDP KANTOR Ltd, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, Final Report, prepared for European Commission, Directorate-General Justice, Freedom and Security, 20 Jan 2010.

http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

cooperation with industrial stakeholders, such as service providers, and are promising in ensuring a higher level of protection for individuals and in raising awareness”.¹⁰

Considering this, we need to understand the significance of privacy seals in greater depth. This is the subject upon which this section focuses.

4.1 GUARANTEE PRIVACY

Privacy seals function as privacy and data protection guarantees. They inform consumers about an organisation’s privacy policies, operations, practices and adherence to certain privacy and data protection standards. They notify consumers about how an organisation may collect, use or share data. They provide “assurance about privacy protection”.¹¹ The European Commission recognises that privacy seals can “give an orientation to the individual as a user of such technologies, products and services”, and are “relevant in relation to the responsibility of data controllers: opting for certified technologies, products or services could help to prove that the controller has fulfilled its obligations”.¹²

Various privacy seals offer a variety of privacy and data protection guarantees. For example, the BBB Accredited Business Seal for the Web offers to guarantee respect for privacy and security for sensitive data, while honouring customer preferences.¹³ The ESRB Privacy Online Program aims to provide data subjects with notice and disclosure, choice, limiting collection and retention of personal information, data integrity and security, data access, enforcement and accountability in terms of the processing of their personal information.¹⁴ Japan’s PrivacyMark system aims to guarantee appropriate protective measures for personal information.¹⁵

Some privacy schemes offer high-level legal privacy and data protection guarantees; others offer only low-level and basic forms of guarantee. EuroPriSe, the only pan-European privacy seal scheme based on EU privacy and data protection law, comprehensively offers to guarantee transparency, a legal basis for processing personal and sensitive personal data, compliance with data protection principles and duties, technical-organisational measures, data subject rights under Directive 95/46/EC and Directive 2002/58/EC.¹⁶ On the other hand, other schemes such as buySAFE Guaranteed Shopping,¹⁷ Gigya SocialPrivacy™ Certification¹⁸ are based on industry developed standards and offer less legally compliant privacy and data protection guarantees.

¹⁰ Council of the European Union, Council conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting, Brussels, 24-25 Feb 2011.

¹¹ Connolly, Chris, “Trust mark Schemes Struggle to Protect Privacy 2008”, Galexia, Version 1.0, 26 September 2008. http://www.galexia.com/public/research/assets/trust_marks_struggle_20080926

¹² 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

¹³ Better Business Bureau, “BBB Accredited Business Seal for the Web”. <http://www.bbb.org/us/bbb-online-business/>

¹⁴ ESRB, ESRB Privacy Online Program. <http://www.esrb.org/privacy/index.jsp>

¹⁵ PrivacyMark. <http://privacymark.org/>

¹⁶ EuroPriSe. <https://www.european-privacy-seal.eu/>

¹⁷ BuySAFE. <http://www.buysafe.com/index.html>

¹⁸ Gigya, Gigya's SocialPrivacy™ Certification. <http://www.gigya.com/solutions/social-privacy/>

Although the level of protection offered might vary, generally, privacy seal schemes aim to guarantee respect for privacy and facilitate privacy compliant actions.

4.2 BUILD AND ENHANCE CONSUMER TRUST AND CONFIDENCE

The overarching objective of privacy seals is to promote and build consumer trust online.¹⁹ There is good recognition of this. According to Bennett and Raab, privacy seals work “to influence, shape or set benchmarks for behaviour in the marketplace”.²⁰ They are visible symbols of trust that provide consumers with privacy assurances²¹ that lead them to act favourably towards a seal holder – i.e., to buy or use products, services or even disclose personal information.²² Marit Hansen states, “The mere existence of the seal demonstrates to users that the providers take their privacy seriously and are willing to invest in data protection and security.”²³

Privacy seal issuers acknowledge the importance of privacy seals in building consumer trust and organisational confidence. The Better Business Bureau (BBB) claims that “Over a million times a month, people click on BBB Accredited Business seals to verify a business' credentials and affirm their commitment to BBB's high standards.”²⁴

Companies using privacy certification also recognise the significant role of privacy seals. ValidSoft, a global supplier of telecommunications-based fraud prevention, authentication and transaction verification solutions has achieved a third seal from EuroPriSe and its chief executive officer (CEO) believes that this helps it “cement” its position “as a global leader in data privacy and protection”, and puts it and its clients “ahead of the game as the mobile/e-commerce market expands”.²⁵ Oracle Vice President for Global Public Policy and Chief Privacy Officer Joe Alhadeff comments,

We consider the TRUSTe seal a key component of our commitment to world-class international privacy standards. Beyond the seal, TRUSTe also delivers significant value as a true business partner in the broader sense, helping to certify, monitor and maintain consistent privacy communications and practices across our many Web sites and throughout our business.²⁶

CISCO Systems Vice President and Law Deputy General Counsel Van Dang claims that “Using the TRUSTe seal is just one more way we can demonstrate to our customers and

¹⁹ Grabner-Kraeuter, S., “The Role of Consumers' Trust in Online Shopping”, *Journal of Business Ethics*, Vol. 39, 2002, pp. 43-50.

²⁰ Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, 2006, p. 122.

²¹ Grabner-Kraeuter, S., “The Role of Consumers' Trust in Online Shopping”, *Journal of Business Ethics*, Vol. 39, 2002, pp. 43-50.

²² Miyazaki, A., and S. Krishnamurthy, “Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions”, *Journal of Consumer Affairs*, Vol. 36, Iss. 1, 2002, pp. 28-49.

²³ Hansen, Marit, “Putting Privacy Pictograms into Practice - A European Perspective” in Stefan Fischer, Erik Maehle and Rüdiger Reischuk (eds.), *Proceedings of GI Jahrestagung*, 2009, pp. 1703-1716.

²⁴ BBB, “BBB Accredited Business Seal for the Web”. <http://www.bbb.org/us/bbb-online-business/>

²⁵ ValidSoft, “ValidSoft achieves unprecedented third European Privacy Seal”, *ValidSoft News*, 13 Nov 2012. <http://www.validsoft.com/news/validsoft-achieves-unprecedented-third-european-privacy-seal-news-23181314243>

²⁶ TRUSTe, “Oracle case study”. <http://www.truste.com/customer-success/oracle/>

employees that we will always do the right thing. And doing the right thing is not only good for our customers — it's the foundation for business success as well.”²⁷

Although privacy seals can be useful instruments to build consumer confidence, one of our advisory board members commented that they should go beyond the legal framework and provide an extra layer of consumer protection. Clearly, some schemes are better than others. The mere presence of a seal is no guarantee that its holder truly does respect privacy rights. If privacy certification schemes are not building an additional layer of protection on top of existing applicable legislation, data subject rights and consumer protection, then the presence of a seal may actively mislead consumers and create false confidence.

4.3 SUPPORT BUSINESS, TRADE AND ECONOMIC GROWTH

By creating and enhancing consumer confidence in an organisation, privacy seals encourage consumers to consume the organisation's products and avail themselves of its services.²⁸ This could boost the organisation's revenues and enhance its economic prospects and support its growth.²⁹ A McAfee data sheet states that the McAfee SECURE trust mark “increases sales conversion by an average of 12%” based on more than 300 A/B tests of the underlying McAfee SECURE technology where one group of consumers was shown the trust mark and the other saw an unmarked site.³⁰

Privacy seals also encourage one business to do business with another – for instance, a data controller may have more faith and find it more acceptable to do business with a privacy-certified data processor (even though there will be degrees of trust depending on the nature of the certification and the applicable compliance standards).

Privacy seals bring added value to small and medium enterprises (SMEs), particularly those that are newly established or are relatively unknown in terms of their credentials.³¹ Privacy certification would help these businesses provide an additional assurance to consumers and users of their services and help build trust and confidence, which in turn will boost business and trade. Cline suggests that, for these types of businesses, “A privacy seal will pay for itself many times over.”³²

²⁷ TRUSTe, “Cisco Systems, Inc.-case study”. <http://www.truste.com/customer-success/cisco-systems/>

²⁸ Cook, David, and Wenhong Luo, “The Role of Third-Party Seals in Building Trust Online”, *e-Service Journal*, Vol. 2, No. 3, Summer 2003, pp. 71-84; Hu, Xiaorui, Zhangxi Lin and Han Zhang, “Myth or Reality: Effect of Trust-Promoting Seals in Electronic Markets”, in Otto Petrovic, Reinhard Posch and Franz Marhold (eds.), *Trust in a Networked Economy*, 2001, pp. 143-150.

²⁹ Miyazaki, A., and S. Krishnamurthy, “Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions”, *Journal of Consumer Affairs*, Vol. 36, Iss. 1, 2002, pp. 28-49.

³⁰ McAfee, “McAfee SECURE Website Certification Leads to Increased Sales”, *Data Sheet*. <http://www.mcafee.com/uk/resources/data-sheets/ds-mcafee-secure-for-websites.pdf>

³¹ A view echoed in relation to trust marks in TNO and Intrasoftware, *EU online Trust marks: Building Digital Confidence in Europe*, A study prepared for the European Commission, DG Communications Networks, Content & Technology, Final report, SMART 2011/0022, 2012.

³² Cline, Jay, “Web site privacy seals: Are they worth it?” *Computerworld*, 8 May 2003. http://www.computerworld.com/s/article/81041/Web_site_privacy_seals_Are_they_worth_it. Jay Cline is a privacy columnist for Computerworld, is the President of Minnesota Privacy Consultants (a privacy consulting company specialising in privacy compliance, healthcare, cloud computing and Europe). He has held leadership positions in the International Association of Privacy Professionals (IAPP) and was a privacy columnist for IAPP's INSIDE 1to1: Privacy.

4.4 FOSTER ADHERENCE TO PRIVACY, DATA PROTECTION STANDARDS

Privacy certification and seals encourage adherence to privacy and data protection values by setting core or baseline standards for compliance by seal subscribers. Privacy seals are soft mechanisms that help to inculcate respect for privacy and data protection values. Though the standards underlying privacy seal schemes vary from provider to provider, O'Connor states that these schemes

encourage companies to behave ethically by providing specific guidelines to insure minimal standards; compelling companies to undergo a review to establish compliance with these standards; requiring companies to submit to periodic re-verification and to commit to a resolution procedure in case of dispute.³³

Privacy seals also foster adherence to privacy and data protection law by embedding such law into its criteria and requirements. For instance, EuroPriSe criteria are based on the European Data Protection Directive (95/46/EC)³⁴ and other EU regulations on data protection, such as the ePrivacy Directive.³⁵ The CNIL label certifies compliance with the French data protection law.³⁶ The ESRB Kids Privacy Certified seal certifies compliance with requirements of the Children's Online Privacy Protection Rule.³⁷

While it might be argued, and even evident from the subsequent analysis of the 25 schemes, that some privately run, industry-led, privacy certification schemes do not strictly or fully meet with privacy and data protection requirements under the existing European data protection framework,³⁸ this does not make such privacy schemes a total failure or irrelevant. For instance, the MRS Fair Data Scheme run by the Market Research Society makes direct reference to the UK Data Protection Act 1998 in addition to other standards schemes such as those of the International Organization for Standardization (ISO), the US Safe Harbor Framework³⁹ and the Data Seal initiative.

³³ O'Connor, Peter, "An International Comparison of Approaches to Online Privacy Protection", in Andrew J. Frew (ed.), *Information and Communication Technologies in Tourism 2005: Proceedings of the International Conference in Innsbruck, Austria*, Springer, Vienna, 2005, pp. 273-284.

³⁴ European Parliament and the Council, Directive 95/46/EC 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, Official Journal L 281, 23/11/1995, pp. 0031 – 0050.

³⁵ EuroPriSe, "Criteria". <https://www.european-privacy-seal.eu/criteria>

³⁶ Commission Nationale de l'Informatique et des Libertés" (CNIL), Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended): <http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf>

³⁷ [US] Federal Register, Children's Online Privacy Protection Rule, Title 16, Chapter I, Subchapter C, Part 312, Washington, DC, 3 Nov 1999. http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title16/16cfr312_main_02.tpl. See also ESRB, "ESRB Privacy Certified Seals". <http://www.esrb.org/privacy/seals.jsp>. The Entertainment Software Rating Board (ESRB) describes itself as "the non-profit, self-regulatory body that assigns ratings for video games and apps so parents can make informed choices".

³⁸ This is further elaborated in sections 6.3.11, 6.3.12, 7.5 and 7.8 of the report.

³⁹ The US-EU Safe Harbor Framework (developed by the US Department of Commerce in consultation with the European Commission) provides "a streamlined means" for US organisations to comply with the EU Data Protection Directive (95/46/EC). See US Department of Commerce, U.S.-EU Safe Harbor Framework http://export.gov/safeharbor/eu/eg_main_018493.asp

4.5 GENERATE PRIVACY ACCOUNTABILITY

Properly implemented privacy seals could help generate privacy accountability. The Article 29 Data Protection Working Party⁴⁰ in its Opinion 3/2010 on the principle of accountability recognises this.⁴¹ It states that privacy seal schemes permit data controllers to prove that they have fulfilled their obligations, implemented appropriate data protection measures and have audit procedures in place. This is based upon the understanding that the schemes' requirements facilitate compliance, with legal privacy and data protection requirements.

Privacy seal schemes require subscribers to adhere to scheme requirements; if scheme requirements are not fulfilled, the seal is liable to be suspended or revoked. This would bring an organisation and its privacy practices into disrepute and may lead to loss of its competitive advantage.

One example of such accountability in practice is TRUSTe's revocation in 2005 of the FreeiPods.com privacy seal belonging to Gratis Internet of Washington, DC, for "unspecified violations of privacy promises to consumers".⁴²

4.6 PROMOTE OVERALL AWARENESS OF PRIVACY AND DATA PROTECTION

Overall, privacy seals promote awareness of privacy and data protection. Hui et al.⁴³ suggest that "In principle, privacy statements and privacy seals help consumers make a more accurate assessment of the risks of disclosing personal information to websites."⁴⁴ This is a useful and important function, particularly given the nature of ever-expanding privacy and data protection threats – such as increased collection, processing and sharing of personal information, expanding surveillance capabilities from existing and new applications.

The online visibility, the prominence on websites, and media coverage of privacy seals and certification (for instance, media releases outlining privacy seal scheme functions and process; issue of seals to various organisations; blogosphere and academic discussions on the merits and demerits of seals) help generate greater awareness of privacy and data protection in society.

⁴⁰ Set up under Directive 95/46/EC and composed of representatives of EU national data protection authorities, a representative of authorities established for the EU institutions and bodies (EDPS) and a representative of the European Commission. See European Commission, Article 29 Working Party. <http://ec.europa.eu/justice/data-protection/article-29/>

⁴¹ Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, WP 173, Brussels, Adopted on 13 July 2010.

⁴² Associated Press, "Privacy-Assurance Seal Yanked", *Wired.com*, 2 September 2005.

<http://www.wired.com/techbiz/media/news/2005/02/66557>

⁴³ Hui, Kai-Lung, Hock Hai Teo and Sang-Yong Tom Lee, "The Value of Privacy Assurance: An Exploratory Field Experiment", *MIS Quarterly*, Vol. 31, Iss. 1, March 2007, pp. 19-33.

⁴⁴ Citing Milne, G.R., and M.J. Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices", *Journal of Interactive Marketing*, Vol. 18, Iss. 3, Summer 2004, pp. 15-29.

4.7 EASY AND QUICK REPRESENTATION OF PRIVACY AND DATA PROTECTION COMMITMENTS

Privacy seals enable organisations to make an easy and quick representation of their privacy and data protection commitments.

Graphics appeal more than text does. In the first instance, privacy seals have an innate ability to easily and quickly present an entity's privacy and data protection commitments. Tan (a Canadian accounting professional specialising in third-party assurance reporting) states, "The main factor that makes privacy seals attractive to websites is the ability to graphically assert something. The ease in which a website would be able to convey an image of trustworthiness to visitors is something that businesses value."⁴⁵

4.8 FLEXIBLE PRIVACY AND DATA PROTECTION MECHANISM

Privacy seals are a comparatively flexible privacy assurance mechanism compared to other mechanisms such as legal regulation. A good privacy and data protection seal scheme is flexible enough to take into account the different natures and requirements of its subscribers. The scheme's requirements or criteria could be tailored to apply to both existing, evolving and new technologies (such as cloud computing, which will be elaborated in Task 3 of the Study) taking into account changing privacy needs and expectations. Privacy seal schemes can quickly meet these changing needs and expectations which might take longer to be embedded into legislation.

4.9 DISPUTE SOLVING MECHANISM

Privacy and data protection schemes provide businesses and users or consumers of their services with quick, inexpensive extrajudicial means of solving disputes in relation to privacy and data protection concerns. This is important given that users and consumers of online services are often global and not restricted to the legal jurisdiction under which the business or entity might fall.

5 CRITERIA FOR EVALUATION AND COMPARISON OF PRIVACY SEALS

This section outlines the criteria used for the evaluation and comparison of the identified certification schemes. The criteria can be divided into two main categories: general criteria and criteria based on the GDPR requirements. The following sub-sections outline the criteria in greater detail. The criteria will then be presented as a collated, comprehensive table (Table 27, Annex I) and used to research selected privacy seal schemes.

5.1 GENERAL CRITERIA

This section identifies and presents the general criteria for analysis and evaluation of the identified privacy seals. The following table lists the criteria:

⁴⁵ However, Tan questions the ability of a seal to achieve this purpose. Tan, Andrew, "Privacy seals", University of Waterloo, 30 June 2011.

<http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Privacy%20Seals%20A%20Tan.pdf>. Tan's study examines the effectiveness of privacy seals such as TRUSTe, WebTrust, their frameworks, and considers their impact on the public accounting profession.

	Criteria for evaluation and comparison of privacy seals	Privacy seal X
1	Nature (privacy-oriented/general trust mark)	
2	Country	
3	Inception	
4	Issuing organisation	
5	Issuer type	
6	Target of scheme	
7	Number of certified entities	
8	Renewals	
9	Types of entities that can be certified	
10	Type of beneficiaries	
11	Objective of scheme	
12	Descriptive summary of scheme	
13	Unique selling point	
14	Privacy/data protection elements of the scheme	
15	Guarantees offered to the data subject	
16	Steps in the certification process	
17	Coverage of international transfers	
18	Costs (i.e., evaluation cost, certification cost)	
19	Validity	
20	Revocation mechanism	
21	Recognition	
22	Accredited experts and/or evaluation bodies	
23	Duration and scope of the certification process	
24	Number of certified experts and/or bodies	
25	Regulatory/ compliance standards	
26	Frequency and means of updates to scheme	
27	Additional elements (e.g., security or other components, links with a privacy program, privacy audits, awareness)	
28	Complaints mechanism	
29	Criticisms	
30	Links and references to the scheme	
31	Logo	
32	Website	

Table 2: General criteria for evaluation of privacy seal schemes

Most of these criteria were specified by the tender call. The following were added to the list specified in the tender: inception, nature, unique features, number of seals issued and renewed (subscribers) and criticisms.

These criteria have been combined with the criteria identified in the following section and used to evaluate the specified privacy certification schemes.

5.2 CRITERIA BASED ON THE GDPR REQUIREMENTS

The European Commission's General Data Protection Regulation in Recital 77 encourages the "establishment of certification mechanisms, data protection seals and marks" to enhance

transparency, legal compliance and to permit data subjects [individuals] the means to make quick assessments of the level of data protection of relevant products and services.⁴⁶

Article 39 deals with certification. It prescribes:

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

This section identifies key requirements from the General Data Protection Regulation that will be used in the analysis of the identified certification schemes. These requirements may be distinguished into two categories: those that incorporate requirements that are also present in the text of the EU Data Protection Directive 95/46/EC and novelties discussed under the draft GDPR currently in the law-making process. The former include, for instance, the general data protection principles such as the fair and lawful collection and processing of data, purpose limitation, accuracy, retention limitation, etc. GDPR-specific novelties include, for instance, the right to data portability, the right to be forgotten, data protection impact assessments and the various implementations of the principle of accountability.

These requirements (which can be used as the guideline for checking the verification procedures for the privacy seals) are listed and explained below:

1. Fair, lawful, transparent processing of personal data

Recital 30 of the GDPR states that “Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned.”⁴⁷ Article 5 (a) specifies that personal data must be “processed lawfully, fairly and in a transparent manner in relation to the data subject”. Article 6 provides the conditions for lawful processing of data.

2. Data collection for specified, explicit and legitimate purposes

Recital 30 of the GDPR states that “the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data”. Article 5 (b) specifies that personal data “must collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”.

⁴⁶ European Commission, COM (2012) 11 final, op. cit., 25 Jan 2012.

⁴⁷ Ibid.

3. *Adequate, relevant and limited data collection*

Recital 30 of the GDPR states that “The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum”. Article 5 (c) specifies that personal data must be adequate, relevant and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data.

4. *Data accuracy*

Recital 30 of the GDPR states “every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted”. Article 5 (d) of the GDPR specifies that personal data must be “accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”.

5. *Time- and purpose-restricted data retention*

Recital 30 of the GDPR states that “to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review”. Article 5 (e) specifies that personal data must be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”.

6. *Data are processed under the responsibility and liability of the controller*

Article 5 (f) of the GDPR specifies that personal data must be “processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation”.

7. *Provision for parental consent based processing of personal data of a child below the age of 13*

Article 8 (1) of the GDPR focuses on the processing of personal data of a child. In relation to the offering of information society services directly to a child, it states that “the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian”. The data controller must make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

8. *Consent requirement for processing of special personal data*

Article 9 of the GDPR focuses on processing of special categories of personal data. Article 9 (1) states:

The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.

This does not apply in cases where the data subject has consented to the processing of her personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

9. Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.

Article 11 of the GDPR focuses on transparent information and communication. Article 11 (1) of the GDPR states that a “controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights”.

10. Intelligible, clear information/communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.

Article 11 (2) of the GDPR states that “the controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child”.

11. Existence of procedures and mechanisms for exercising the rights of the data subject

Article 12 of the GDPR deals with procedures and mechanisms for exercising the rights of the data subject. Article 12 (1) states:

The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

12. Provision for communication of rectification or erasure carried out under Articles 16 and 17

Article 13 of the GDPR (rights in relation to recipients) states that “the controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort”.

13. Provision of information to the data subject

Article 14 of the GDPR deals with information to the data subject. It states:

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:
 - (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;
 - (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of

- Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
- (c) the period for which the personal data will be stored;
 - (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;
 - (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

14. Provision for right of access for the data subject

Article 15 of the GDPR deals with the right of access for the data subject. It states that a data subject “shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed”. Further,

the data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

15. Provision for right to rectification

Article 16 of the GDPR focuses on the right to rectification. According to it, data subjects shall have the “right to obtain from the controller the rectification of personal data relating to them which are inaccurate” and the “right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement”.

16. Provision for right to be forgotten and to erasure

Article 17 of the GDPR incorporates the right to be forgotten and to erasure. Accordingly,

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
 - (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
 - (c) the data subject objects to the processing of personal data pursuant to Article 19;
 - (d) the processing of the data does not comply with this Regulation for other reasons.

The GDPR Explanatory Memorandum explains that

Article 17 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology “blocking”.

17. Provision for right to data portability

Article 18 of the GDPR incorporates the right to data portability. According to this provision, a

data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

18. Provision for data subject's right to object

Article 19 of the GDPR provides a right to object. A data subject has the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

19. Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)

According to Article 19(2) of the GDPR, “where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing”. This right is to be “explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information”.

20. Rights in relation to automated processing

Article 20 focuses on measures based on profiling. It states:

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

21. Documentation requirements

Article 28 of the GDPR outlines documentation requirements for controllers and processors. It states:

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.
2. The documentation shall contain at least the following information:
 - (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
 - (b) the name and contact details of the data protection officer, if any;
 - (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

- (d) a description of categories of data subjects and of the categories of personal data relating to them;
- e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
- (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
- (g) a general indication of the time limits for erasure of the different categories of data;
- (h) the description of the mechanisms referred to in Article 22(3).

22. Implementing the data security requirements

Article 30 of the GDPR deals with security of processing. It states:

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

23. Notification of a personal data breach to the supervisory authority

Article 31 of the GDPR prescribes a notification requirement in relation to personal data breaches. If there is a personal data breach, a controller must “without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority”. This notification must be accompanied by a reasoned justification if it is not made within 24 hours.

24. Communication of a personal data breach to the data subject

Article 32 deals with communication of a personal data breach to the data subject. It states:

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).

25. Data protection impact assessment

Article 33 of the GDPR focuses on data protection impact assessment:

Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

26. Compliance with the requirements for prior authorisation/prior consultation of the supervisory authority pursuant to Article 34(1) and (2)

Article 34 of the GDPR calls for prior authorisation and prior consultation. Article 34 (1) states:

The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

Article 34 (2) states:

The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

- (a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or
- (b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

27. Designation of a data protection officer

Article 35 deals with designation of the data protection officer. It requires controllers and processors to designate a data protection officer in the following cases:

- (a) the processing is carried out by a public authority or body; or
- (b) the processing is carried out by an enterprise employing 250 persons or more; or
- (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

28. Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations

Article 22 (3) of the GDPR states that the controller must implement mechanisms to ensure the verification of the effectiveness of measures outlined in Article 22 (1) and (2) (i.e., data processing, data protection impacts assessments and data security). Further, “If proportionate, this verification shall be carried out by independent internal or external auditors”.

The following table presents the extracted requirements that will be used for each privacy certification scheme analysis:

General data protection regulation requirements under	Privacy seal
---	--------------

Chapters II and III		
1	Fair, lawful, transparent processing of personal data	
2	Data collection for specified, explicit and legitimate purposes	
3	Adequate, relevant and limited data collection	
4	Data accuracy	
5	Time and purpose restricted data retention	
6	Data is processed under the responsibility and liability of the controller	
7	Provision for parental-consent-based processing of personal data of a child below the age of 13	
8	Consent requirement for processing of special personal data	
9	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	
10	Intelligible, clear information/communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child	
11	Existence of procedures and mechanisms for exercising the rights of the data subject	
12	Provision for communication of rectification or erasure carried out under Articles 16 and 17	
13	Provision of information to data subject: <ul style="list-style-type: none"> • Identity and the contact details of the controller • Purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	
14	Provision for right of access for the data subject	
15	Provision for right to rectification	
16	Provision for right to be forgotten and to erasure	
17	Provision for right to data portability	
18	Provision for data subject's right to object	
19	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	
20	Rights in relation to automated processing	
21	Documentation requirements (Article 28)	
22	Implementing the data security requirements (Article 30)	
23	Notification of a personal data breach to the supervisory authority (Article 31)	
24	Communication of a personal data breach to the data subject (Article 32)	
25	Data protection impact assessment (Article 33)	
26	Compliance with the requirements for prior authorisation/prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	
27	Designation of a data protection officer (Article 35(1))	

28	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations (Article 22)	
----	--	--

Table 3: GDPR requirements-based criteria for evaluation of privacy seal schemes

5.3 COLLATED CRITERIA

The collated criteria (including both tables presented in sections 5.2 and 5.3) are presented in the collated scheme assessment table in Annex I (Table 27).

6 IDENTIFICATION AND ANALYSIS OF PRIVACY SEAL SCHEMES

This section identifies and analyses privacy seal schemes in the 28 EU Member States as well as prominent international schemes. The study team analyse schemes, such as EuroPriSe,⁴⁸ developed under the EU research programmes. The team collected information about the schemes through a variety of means – desktop research, telephone interviews and correspondence with relevant companies or organisations. This research was carried out between 1 April 2013 to 30 June 2013 and the analysis in this report is based on the information collected and analysed during that period.

6.1 LIST OF PRIVACY SEAL SCHEMES

There is a range of privacy and data protection schemes across the 28 EU Member States and worldwide. This report contains an analysis of the following schemes:

1. BBB Accredited Business Seal
2. buySAFE Guaranteed Shopping
3. Cloud Security Alliance
4. CNIL label
5. Comodo Secure
6. Confianza Online
7. Danish e-mark
8. ePrivacyseal
9. ESRB Privacy Online Certification
10. Euro-label
11. EuroPriSe (European Privacy Seal)
12. Gigya's SocialPrivacy™ Certification
13. Market Research Society (MRS) Fair Data
14. McAfee Secure
15. PrivacyMark System
16. Privo Privacy certified
17. Seriedad Online
18. Smart Grid Privacy Seal
19. Transaction Guard Privacy Policy Verified Seal
20. TRUSTe
21. Trusted Shops
22. Trustify-Me Privacy Certification Seal

⁴⁸EuroPriSe. <https://www.european-privacy-seal.eu/>

23. TÜV privacy seal
24. Verified by Visa
25. WebTrust

Many of these schemes are not purely privacy or data protection certification schemes; they are general trust marks incorporating some elements of privacy and data protection (for instance, how information is collected and processed, obligations of companies processing personal data).

6.2 THE RESEARCH SCOPE, LIMITATIONS AND PROBLEMS

The main source of information on the individual certification or seal schemes was the seal issuer's own website. To get an in-depth and more comprehensive understanding of the schemes, the researchers approached the certification schemes mainly from two parallel directions – one, as a potential certification scheme member or buyer, to understand what information was available this way; two, as a user of the scheme's website looking for information on the scheme in general and to verify issued seals. Where information was not available on the website, the study team made specific targeted requests for information to the seal provider.

The study team sought criticisms of the various privacy seals schemes, based on the assumption that any new European privacy seal scheme should avoid being attacked for weaknesses evident in other schemes. To this end, the study team by conducted Web searches with the seal name (or variants such as provider name) alongside keywords such as “concern”, “criticisms”, “dangers”, “fraud”, “insecure”, “issues”, “problem”, and “scam”. The searches focused upon the trade and technical press as well as the academic sources and included some information found in online forums. These were particularly sites that Web users and small business searched to determine if a particular seal was worth buying or subscribing to.

The key problems encountered while finding information on the individual privacy seal schemes are listed below.

6.2.1 Lack of availability and easy accessibility to information

One of the main problems encountered during the research related to the availability of information. General information was not available or easily accessible for some of the schemes from their websites. Though each scheme analysed had a web presence, the depth, quality and ease of accessibility of these varied. Some web pages acted as little more than a shop front for a potential member of the seal scheme. In one case, a web site did not even provide contact information for the seal scheme.⁴⁹ Often seal websites would provide basic or abstracted information about the aims of the seal, for example “helps you stay safe online”, rather than specific information about the functioning of the scheme.

In general, the more commercially focused a seal was or the more it resembled “seal as a service”, the harder it was to find specific details about the scheme, potentially because some of the information (on costs, etc.) might be negotiable.

⁴⁹ For example, Trustify-Me Privacy Certified. <http://trustify-me.org>

Some of the scheme websites are not very user friendly: information had to be sourced from various different parts of the scheme's website. Though many of the schemes had a section for Frequently Asked Questions (FAQs), these were often not very clear or comprehensive. There was generally little information on the limitations of any of the schemes.

It was also difficult to find information (of a more comprehensive nature) on some certification schemes such as the Danish e-mark. However, all efforts were made to gather the relevant information using different means and this has had a minimal impact on the results of the study.

6.2.2 Difficulty finding the specific criteria or requirements for award of seals

While a majority of certification schemes (such as EuroPriSe, TRUSTe, Trusted Shops, WebTrust, etc.) did publicise and present their criteria, there were other certification schemes that did not publish the criteria or requirements and standards for award of seals on their main website. In the case of PRIVO, the terms for use of the privacy seal were obtained from the published documents of an application by PRIVO for recognition from the U.S Federal Government, which had more open publication processes. Transaction Guard has no criteria on its website, specifying only that "its experts draft a Privacy Policy for the websites undergoing the certification process. The policy is intended to be "100% compliant with all the major search engines such as Google, Yahoo, MSN, etc."⁵⁰

The programme requirements for the Smart Grid Privacy Seal are not available on their website; although the programme requirements for their other seals were present (there was a web page link to programme requirements, but this directed the visitor to an incorrect page).

All this made it rather challenging to find information and in particular to evaluate each scheme's criteria or standards in relation to the General Data Protection Regulation categories.

6.2.3 Lack of response to information requests

Specific and targeted requests for information were made during April and June 2013 to some scheme issuers. A couple responded positively (TÜViT and MRS Fair Data), provided clarifications and sent information documents. However, other requests for information were only partially successful (as in the case of Confianza Online and the Seriedad Online) or not successful at all. Despite several requests for information to the Danish e-mark issuing body, no response was received at all. There was also no response from McAfee about lack of program requirements (via email and Twitter).

6.2.4 Necessity of relying on second and third party information

The problems outlined above inevitably resulted in the need to rely on second and third party information. For instance, as information about the pricing of the McAfee Secure scheme was

⁵⁰ Transaction Guard, Privacy Policy Verified Seal. <http://www.transactionguard.com>

not available on its website, the study team sourced information from the scheme's resellers and partners' websites. The team found information on some of the requirements for the Smart Grid Privacy seal program on the website of the Future of Privacy Foundation, which worked with TRUSTe in setting up the scheme.

The study team has used information from second and third-party sources very exceptionally and mentioned specifically where that is the case.

6.2.5 Language barriers

Some of the certification schemes did not provide any information, or provided only limited information on their websites in a language other than the language of the provider. This was the case with the Danish e-mark, Confianza Online and Seriedad. Attempts to contact these schemes through e-mail were only partially successful. Confianza Online amended their website, but the Danish e-mark provider did not reply. Given the time and resource constraints, the research made use of automated online translation services in order to access information about these certification schemes.

6.2.6 Non-availability of certain schemes

The privacy seals inventory (i.e., the 25 schemes listed for analysis) excludes i-Privacy (Australia), Portugal's PACE, PrivacyBot, and TrustUK, mentioned in the tender call and the proposal. 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.⁵¹ For TrustUK, other than some third-party information dating back to 2002⁵², it has not been possible to find a website or first-hand information. These were replaced with: ePrivacyseal, Gigya's SocialPrivacy™ Certification, Market Research Society (MRS) Fair Data, PRIVO's Privacy certified and Trustify-Me Privacy Certification Seal. Data was also not available for Garantia Proteccion des Datos (links to the scheme do not work); this was replaced by Seriedad Online⁵³ which seems to have strong data protection elements. Research and enquiries revealed that the European Privacy Trust mark scheme was not functional yet (in anticipation of the General Data Protection Regulation).⁵⁴ The Transaction Guard Privacy Policy Verified Seal is analysed instead.

6.2.7 Name changes

Another problem noted in connection with the research into certification schemes was changes in the names of schemes. For instance, McAfee HackerSafe became McAfee Secure - this makes finding information and understanding the scheme more problematic. It is not entirely transparent what other details of the scheme changed during this rebranding.

6.2.8 Lack of discussion of the GDPR

⁵¹ Caslon Analytics, "Trust marks". <http://www.caslon.com.au/trustmarksprofile2.htm>

⁵² Consumer and Business Affairs Victoria, Department of Justice, "Web seals of approval", January 2002. <http://www.consumer.vic.gov.au/library/publications/resources-and-education/research/web-seals-of-approval-2002.pdf>

⁵³ Seriedad Online. <http://www.seriedadonline.es/>

⁵⁴ Confirmed via personal communication from a European Privacy Association team member to the study team.

Finally, none of the schemes researched made any explicit reference to the General Data Protection Regulation. This is not surprising given that many of the schemes (such as BBB Accredited Business Seal, buySafe Guaranteed Shopping, Cloud Security Alliance, ESRB Privacy Online Certification, Gigya's SocialPrivacy™ Certification, PrivacyMark system, Smart Grid Privacy Seal, Transaction Guard Privacy Policy Verified Seal and TRUSTe) originate outside the EU. This meant that completing the GDPR categories of the research required a deeper understanding how the scheme worked and finding applicable requirements that overlapped or paralleled with the GDPR categories, or would contribute towards them. For instance, none of the US-based schemes used language relating to the “rights” of data subjects, but some did allow for the correction of errors or offer routes for access to personal data. Several also included a security element, which would contribute towards meeting information security requirements under the GDPR categories. Section 6.4 presents the results of this analysis against GDPR criteria, as well as further explanations of the absence of GDPR criteria in the analysed schemes.

6.3 ANALYSIS OF PRIVACY SEAL SCHEMES AGAINST GENERAL CRITERIA

This section presents the results of the analysis of the identified privacy seal schemes against the criteria set out in section 5.1.

6.3.1 Nature

The schemes analysed can be divided in four broad categories based upon their nature. For the purposes of this report, we can divide the schemes into categories that reflect their role in the personal information ecosystem, and the way their combination of aims, objectives, intended audience, and the type of claims the scheme makes are connected together to produce a functioning scheme.

Nature	Examples
General trust marks	BBB Accredited Business Seal, CSA, Confianza Online, Danish e-mark, Euro-label, Seriedad Online
Privacy and data protection schemes	CNIL label, ePrivacySeal, ESRB, EuroPriSe, Gigya, Fair Data, PrivacyMark, PRIVO, Smart Grid, PrivacyMark System, Transaction Guard, TRUSTe, Trustify-me, TÜViT Trusted Site Privacy, WebTrust.
E-commerce schemes	buySAFE, Trusted Shops, Verified by Visa
Security provider seals	Comodo, McAfee SECURE

Table 4: Nature-based classification of schemes

General trust marks represent schemes with broad and more inclusive, rather than specific, objectives, such as facilitating trust in e-commerce. Underlying these schemes is a broader range of criteria (such as security or privacy). These trust marks make more general assertions about certified entities.

Privacy or data protection schemes make specific claims about the privacy and personal information processing commitments and practices of the scheme members. Some privacy certification schemes are particular versions or offshoots of broader trust mark schemes.

E-commerce schemes focus upon the integrity and reliability of commercial transactions.⁵⁵ These can include the information security element of the financial transfer, as well as guaranteeing the quality of the product, the reliability of the shipping or adding insurance products to the commercial process.

Security provider seals signify that a website uses a particular information security provider's services. Rather than assert that a site's security processes meet a particular standard, the security provider actively provides those security processes and technology.

6.3.2 Country

The following table shows the geographical location of scheme operators.

Region or country	Schemes
Global	Trustify-me, Verified by Visa
United States (international)	Cloud Security Alliance, ERSB, TransactionGuard, TRUSTe, Gigya, McAfee Secure
United States (domestic ⁵⁶)	BBB Accredited Business Seal, buySAFE, Smart Grid Privacy Seal, WebTrust, PRIVO
Canada	WebTrust
Europe	Euro-Label ⁵⁷ , EuroPriSe
France	CNIL label
United Kingdom	Comodo, MRS Fair Data
Spain	Confianza Online, Seriedad Online
Denmark	Danish e-mark
Germany	ePrivacyseal, Trusted Shops, TÜViT Trusted Site Privacy, EuroPriSe
Japan	PrivacyMark System

Table 5: Geographical location of scheme operators

Of the schemes analysed, the vast majority are based in the United States, with a roughly even split between those addressing a domestic and an international audience. Collectively, Europe has a large number of schemes (especially as European websites also have access to the international seals based in the US). However, there are a large number of schemes aimed at individual Member States rather than a collective European audience. Two schemes, Euro-Label and EuroPriSe, attempt to offer a pan-European seal. The Euro-Label scheme (a co-operative trust marks initiative between national suppliers of Internet trust marks in Germany, Austria, Poland, Italy, Spain and Ireland) has a collective common minimum standard (The European Code of Conduct).⁵⁸ However, the scheme is currently only active in Germany and Austria. EuroPriSe is a privacy certification scheme targeted at manufacturers and vendors of IT products and IT-based services, and run by the Unabhängiges Landeszentrum für Datenschutz (UDL), the data protection authority of the German Land of Schleswig-Holstein.

⁵⁵ Anetcom, Garantías de navegación segura: Análisis de los sellos y códigos de confianza en comercio electrónico, ERDF, Valencia, 2013. http://video.anetcom.es/editorial/guia_navegacion_segura.pdf

⁵⁶ US-based schemes targeted at domestic US websites and services.

⁵⁷ Though this scheme claims to have a European scope, it is currently only active in Germany and Austria.

⁵⁸ Euro-Label. <http://www.euro-label.com/en/code-of-conduct/index.html>. According to the website, "Each supplier uses its own list of criteria that surpasses the minimum requirements of the collective Code of Conduct and meets specific national features."

Global (international and US-based) seals tend to be based upon corporate models and set up by private sector actors. The exception to this is the Entertainment Software Rating Board (ESRB), which is a non-profit, self-regulatory body administering the ESRB privacy certification scheme. Privately administered seals, negotiated and delivered on a commercial basis, seem to be marketable to the Internet generally. Additionally, seals based upon a code of practice or programme requirements created solely by the certifying body, rather than based upon national law, seem to have wider spread.

Seals produced by organisations at national level, such as the CNIL label (and those based upon recognising compliance with a particular legal standard), tend to have a strongly delineated geographic boundary that matches the remit of the organisation. There is a lesser incentive for a website or service provider outside these jurisdictions (or not intending to operate within them) to participate in one of these schemes.

6.3.3 Inception

The following graphic sets out the inception timeline for the analysed schemes:

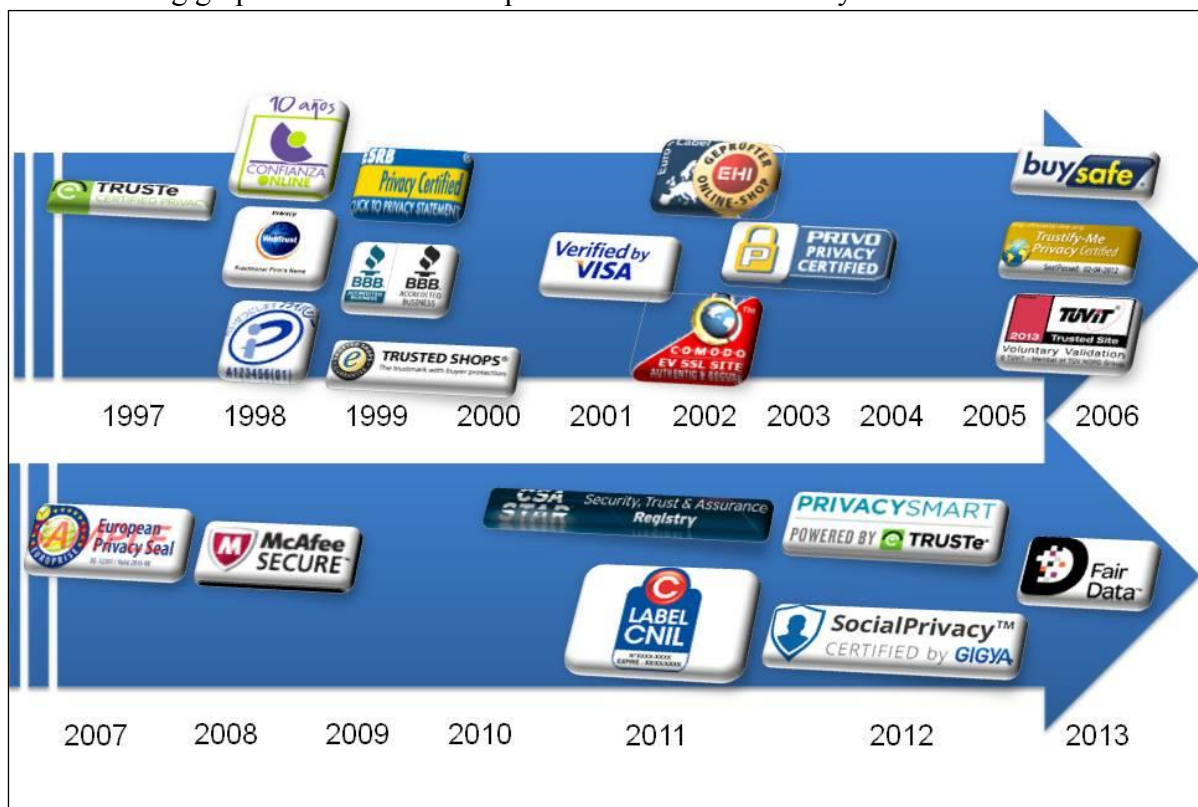


Figure 1: Inception timeline

Figure 1 plots the inception dates (where available) for the analysed schemes by year. The study identified three main “waves” of seals. Not all of the seals analysed fit neatly into these waves, and there is an overlap between the waves, but the separation does provide some analytical leverage.

First wave: Traditional broad-spectrum trust marks

The first wave in relation to the analysed schemes is the emergence of traditional broad-spectrum trust marks. This period starts in 1997. This wave includes schemes focused on privacy and the proper handling of personal information (TRUSTe, ESRB Privacy Certified, Japanese PrivacyMark, and WebTrust). The main characteristic of this wave (and schemes that come within it) is a broad applicability across technological or industry segments. The first wave continues with occasional new market entrants with similar models. Some of the early schemes were also built around the provision of seals on printed material as well as websites, whereas later schemes were targeted more at an online audience. The first wave sets the general model for seal schemes, with subsequent entrants imitating these models very closely.

Second wave: Trusted shopping

The second wave of seals, emerging from 1999 to 2006, includes schemes focused on providing a safe and secure online commerce experience. They are focused on persuading website visitors that the website is a safe and trustworthy place to shop, that they will receive the product they pay for and their credit card details will not be stolen. These trusted shopping schemes do not have a strong focus on privacy or data protection, beyond potentially the prevention of identity or card fraud. Examples include the Better Business Bureau scheme, Trusted Shops, Verified by Visa and buySafe.

Third wave: Specialised seals

From 2011 onwards, privacy and data protection certification schemes aiming at a niche or specialised segment of the market start to emerge more prominently. This may be a sign that the certification schemes market is segmenting from a broader approach to a more targeted approach, that there are increasingly specific sets of privacy or information processing concerns, or that certification scheme operators see a potential gap and market for such schemes as opposed to general trust mark schemes.

The Cloud Security Alliance (CSA), a register of the security controls of cloud service providers, was launched in 2011.⁵⁹ Gigya Inc. launched its SocialPrivacy scheme in 2012 targeted at the niche area of social log-ins.⁶⁰ Social log-in involves users logging into websites using their social network credentials, and makes claims that certified entities will not sell on information obtained through that log-in, send private messages to a user's friends and/or post publicly on behalf of the user, unless directed. Social log-in is a relatively new process, and one with a particular set of privacy concerns, given that a single set of credentials may link behaviour and activity across a wide range of websites. Similarly, the Smart Grid Privacy Seal is an offering from TRUSTe and The Future of Privacy Forum specifically targeting companies seeking to use customer energy use data produced by smart energy meters.⁶¹ Neither of these specialised schemes is the sole product offered by CSA, Gigya Inc. or TRUSTe. Although the Market Research Society (MRS) Fair Data mark could be considered a specialist seal given its focus, unlike the others in this wave, it is not targeted at a particular

⁵⁹ Cloud Security Alliance. <https://cloudsecurityalliance.org/star>

⁶⁰ Gigya, Inc., www.gigya.com

⁶¹ The Future of Privacy Forum, Smart Grid. www.futureofprivacy.org/issues/smart-grid/

industry or set of related technologies.⁶² It targets both public and private sector organisations collecting and using personal data.

6.3.4 Issuing organisation and issuer type

The following table shows the nature of the organisations issuing the analysed certification schemes.

Type of organisation	Schemes
Private company	buySAFE, Comodo, ePrivacyseal, SocialPrivacy (Gigya), McAfee, PRIVO (Privacy Vaults Online), Seriedad Online, Smart Grid, Transaction Guard, TRUSTe, Trusted Shops, Trustify-me, TÜViT Trusted Site Privacy, Verified by Visa, WebTrust
Data protection authority	CNIL Label, EuroPriSe
Not-for-profit, non-governmental organisation	BBB Accredited Business Seal, Cloud Security Alliance, Confianza Online, Danish e-mark (the e-Commerce Foundation), ESRB, Euro-Label, the PrivacyMark System.
Professional representative body (industry association)	Fair Data (Market Research Society)

Table 6: Organisation-based categorisation of schemes

Only two schemes are administered by data protection authorities: the CNIL label (France) and EuroPriSe (administered by the Unabhängiges Landeszentrum für Datenschutz (ULD) of Schleswig-Holstein). No schemes are directly administered by national governments or by intergovernmental bodies.

6.3.5 Target of scheme and entities that can be certified

For many of the analysed schemes, the categories “Target of schemes” and the “Type of entities that can be certified” overlapped. Whilst this is to be expected, it does show how the language used by the schemes to explain themselves, their standards and processes in any detail is primarily targeted at the certified entity, not at the consumer, data subject or end user. To use a market analogy, the end user is a “product” delivered to the certified entity, not primarily a decision-maker. It is possible to make a distinction between broad and narrow schemes. The broadest schemes appear to be willing to include any website that meets their programme requirements.

Target Category	Sub-category distinctions	Schemes
Organisational	Geography	BBB Accredited Business Seal, buySAFE, PrivacyMark System, ESRB EU Privacy Certified
	Business type	CSA, Smart Grid, Verified by Visa
	Private organisations	All

⁶² MRS, “Fair Data: Launch of personal data mark set to rebuild public trust”. <https://www.mrs.org.uk/article/item/696>

	Public & Private	Confianza, MRS Fair Data
Individual website	Type of service	Trusted Shops
	Audience	Privo
Systems		EuroPriSe
Web users		

Table 7: Targets and schemes

The main categories of entities certified are organisational, individual websites and systems. One major distinction for privacy seal schemes is between schemes that certify the information-processing and data protection practices of an entire company or organisation and those that only certify one particular website of a company. The distinction is important because a single company could host multiple websites (for instance, Sony Entertainment or Pokemon)⁶³ that have privacy and data protection impacts (i.e., the company could have only one privacy-certified website but might collect and use personal data on its other uncertified sites). Additionally, an organisation might conduct significant processing of personal information for its core business, but conduct very little collection and processing of personal information through its promotional website. If a seal certifies the company rather than the website, the seal might be potentially misleading.

For seals that certify the practices of an entire organisations, the main distinctions were based upon geography (BBB Accredited Business Seal, buySAFE, PrivacyMark System, ESRB EU Privacy Certified) or upon business type (CSA, Smart Grid Privacy seal, Verified by Visa). The most commonly specified target in this area was online retailers (for e-commerce seals). Most of the seals in this category were addressed to private companies; however, Confianza and MRS Fair Data also target public organisations. Verified by Visa is the only seal which specifies that it certifies banks and card issuers.

For seals certifying individual websites, the primary distinctions were between websites offering particular types of services (Trusted Shops certifies websites with a fully online payments process), websites catering to specific audiences (PRIVO certifies websites aimed at, or likely to be collecting personal data on, children under 13), or excluding particular categories of website (McAfee SECURE excludes competitors, convicted computer criminals, websites in regions prevented by law and websites with defaulted accounts). McAfee Secure can be set up for websites, domains, individual IP addresses and pages. Whilst it is always organisations that process personal data, several of the seal schemes appear to focus upon the particular processing practices associated with a particular web offering. This is a significant limitation and could be potentially misleading for users.

A small number of analysed schemes focus on the certification of systems beyond websites. EuroPriSe, for instance, can certify particular products, services, sets of related products and particular technologies. To the extent that information processing and data collection are increasingly occurring through networked devices, smart and ubiquitous technology, this is likely to become a developing area for seal schemes. The extent to which the website model, or indeed the concept of a single certified organisation conducting data processing, can apply is potentially questionable. For example, imagine a utility company running a set of smart meters collecting data in consumers' homes, having a central data processing operation, and a customer-facing website. Does a privacy seal on the website of this company cover the company's entire privacy practices or just those used on the website (which may be minimal

⁶³ ESRB, "Websites certified by ESRB Privacy Online". <http://www.esrb.org/privacy/sites.jsp>

and limited to providing information to website visitors) and what can the customer reasonably believe from seeing this seal?

The promotional material for several of the analysed schemes (BBB Accredited Business Seal, buySAFE, CNIL label, Verified by Visa) suggested that the schemes were targeted (at least in part) at web users and online shoppers. However, the primary targets for these schemes must be considered to be the certified entities, given that these primarily bear the costs associated with certification and seals provision. The majority of schemes primarily address themselves to potential certified entities as a way to demonstrate their practices to their customers.

6.3.6 Number of certified entities

The following table shows data uncovered in researching the number of entities certified by each scheme.

Analysed schemes	Number of certified entities
Verified by Visa	300,000 websites (in Europe)
BBB accredited business seal	145,700 websites
McAfee Secure	80,000 +
PrivacyMark	15,667
Trusted Shops	15,046
buySAFE Guaranteed Shopping	> 5000
TRUSTe	5000 clients
Confianza Online	2,556
ESRB	2,000
Danish e-mark	1,475
Euro-Label	906
Cloud Security Alliance	29
Seriedad Online	28
PRIVO Privacy Certified	26
EuroPriSe	24
MRS Fair Data	17
TÜViT Trusted Site Privacy Certification	12
CNIL label	20
ePrivacyseal	10
Gigya Social Privacy	6-12 (but potentially large social networks)
Trustify-me	< 5
SmartGrid Privacy seal	~ 3
Comodo Secure	Unknown
Transaction Guard	Unknown
WebTrust	Unknown

Table 8: Number of certified entities

These data were sourced from the scheme websites, the scheme operators' promotional material and annual reports and was collected between 1 April 2013 and 30 June 2013. We recommend checking the individual scheme websites for the current figures.

The rough number may be misrepresentative, given that some members of these schemes are very significant websites with large numbers of users and high traffic. For example, Gigya's

SocialPrivacy certification which has a small number of certified entities asserts that it is currently working on certification for organisations such as Facebook, Yahoo, Twitter, LinkedIn and other significant social networks.⁶⁴ Numbers include the launch partners: Martha Stewart Omnimedia, LUSH cosmetics, Finish Line, *The Globe and Mail*, Facebook, Twitter, LinkedIn, Google, Yahoo, and Windows Live Messenger.

Factors correlated with having a large number of certified entities include being able to mandate participation or to apply penalties for non-participation. For example, VISA's central position in the payments infrastructure, and its offer to participating merchants to reduce the charges associated with non-authorised transactions, as well as the bundling of Verified by Visa with online payments systems, means that Visa has been able to spread its scheme widely.

The specialist and niche seal schemes appear to cluster between 26 and three participants. This may represent the scale of these individual sectors combined with the relative novelty of specialist seals.

The following table illustrates the number of entities certified by the analysed schemes according to organisation type:

Type of certifying entity	Number of certified entities
Company	405,142
Governmental organisation	44
International governmental organisation	0
Not-for-profit, non-governmental organisation	168,333
Professional representative body	17

Table 9: Number of certified entities by organisation type

The following table presents the number of entities certified by the analysed schemes according to nature of seal:

Nature of seal	Number of certified entities
General trust marks	150,694
Privacy/data protection	22,786
E-commerce	320,046 ⁶⁵
Security providers	80,000

Table 10: Number of certified entities by nature of seal

6.3.7 Validity and renewals

Very little information was available on the validity periods and renewal of the analysed schemes. For instance, there was no information provided on how regularly buySAFE updates its assessments of eligibility. Information on validity and renewals is important because it allows the relying party to evaluate how long it might have been since the last audit or certification process. Given that privacy and data protection processes, as well as information

⁶⁴ Gigya, Inc., Privacy Program Requirements. <http://www.gigya.com/solutions/social-privacy/program-requirements/>

⁶⁵ The 300,000 websites in Europe claimed by Verified by Visa are responsible for the majority of this figure.

security practices, can change and even become ineffective over time, a long renewal process increases the likelihood of a website featuring an inappropriate or misleading seal. Several schemes suggest they conduct “periodic” re-certification and audits, without specifying the timescales involved. EuroPriSe specifies that it conducts mandatory monitoring eight and 16 months into the seal’s validity.

Where periods of validity and renewal are specified, one year is the most common renewal period. PRIVO Privacy Certified and the CSA scheme require annual self-assessments to maintain validity. PRIVO supplements this with quarterly reviews, “periodic” unannounced checks and community monitoring. The CSA marks registry entries older than a year as deprecated and removes them completely after an additional six months. Several commercial schemes have monthly renewals (BuySAFE, McAfee Secure, Comodo) based on continuing monthly payments. Some schemes allow a customer to select to pay monthly or yearly, with a discount for longer contract lengths.

TÜViT’s Trusted Site Privacy certification mark, EuroPriSe and the Japanese PrivacyMark schemes have a two-year validity period. The Japanese PrivacyMark allows for a two-year extension after the initial validity period. After that, the seal needs to be renewed every two years. The CNIL label has the second longest validity, remaining valid for three years, although with the obligation of providing an annual report, and renewable up to six months before expiry.

McAfee Secure has the most frequent renewal and shortest period of validity. McAfee’s information security vulnerability scan checks client websites daily for any unpatched vulnerabilities. The McAfee client is informed of the vulnerability and remedial measures. Verified by Visa requires re-certification and testing following any changes to the websites’ payments software or changes to payments providers.

Where information on renewals and validity was provided, many schemes stated that their seal became valid immediately following the initial certification process, often after signing a licence agreement or contract. For instance, Verified by Visa is valid once the appropriate software is installed, tested and the licence agreement is signed with the service provider.

6.3.8 Types of beneficiaries

The vast majority of analysed schemes identify “consumers” as a key beneficiary. Only schemes certified by data protection authorities identify citizens or the public as beneficiaries (CNIL label and EuroPriSe). Variants on “consumer” included “online consumer” and “Internet consumer”, but this should not be taken to represent a lack of focus on online commerce in other schemes. The second most common way of referring to individual beneficiaries was as “users”, primarily e-commerce users, website or Internet users.

Nearly all the analysed schemes identify benefits for the certified entity (in a majority of cases, this envisaged a business). In most cases, the certified entity decided if pursuing certification was supported by a business case, and the benefits cited range from generally improving trust and confidence to making specific increases in e-commerce sales.

Some of the relative focus or breadth of the analysed schemes is identifiable by whom the scheme beneficiaries are. Broad schemes identify “Internet users” or “customers”, whilst more specialised schemes target specific beneficiaries. For example, the CSA scheme benefits

cloud service customers. PRIVO Privacy Certified benefits children under 13 and their parents. The ESRB EU Privacy Certified seal would benefit companies doing business with EU-based consumers.

A more in-depth analysis of beneficiaries, benefits and impacts is provided in Section 8.

6.3.9 Objectives of the scheme

The analysed schemes cluster around a number of similar and overlapping objectives. These are:

To build confidence and trust

This generally refers to building the confidence of users and visitors with regard to a particular website. Confidence (and trust) are sometimes related to particular measures such as data protection, security or guaranteed transactions, but are also frequently left abstract, referring to a general sense of confidence in a website and “peace of mind” (Trusted Shops). The goal of helping consumers shop can also be understood in terms of commercial confidence. Building trust is closely related to building confidence, and often used interchangeably. Several schemes suggest that the presence of the seal increases the trust website visitors have in the website. Trust and confidence are closely related to commercial opportunities.

To signal compliance or accordance with standards

Standards may be derived from the seal scheme itself or may demonstrate compliance with a code of practice or law. The CNIL label demonstrates compliance with the French Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties. PRIVO demonstrates that a site meets or exceeds the United States’ Children’s Online Privacy Protection Act guidelines, whilst Seriedad Online signals compliance with the Spanish Organic Law on Data Protection (Data Protection Act, Act 15/1999 of December 13, Protection of Personal Data), and Law of Services of the Information Society and Electronic Commerce (LSSICE, Law 34/2002 of July 11 effective from October 2003). Schemes that focus compliance with their internal standard or code of conduct seem more likely to make this publicly available than the programme requirements of schemes focused upon consumer confidence. A related form of this objective is Smart Grid Privacy Seal’s objective of simplifying third-party vetting in the customer energy use data market.

To signal data protection measures

Rather than signalling compliance with a standard or code of practice, these seals aim to signify that a set of particular data protection or security measures are in place. TRUSTe’s focus upon data protection puts it into this category. McAfee Secure and Verified by Visa seals are tightly linked to technical security measures. The Trustify-me and ESRB schemes suggest they notify members of any potential data protection issues and remedial measures as part of their certification process.

To provide guarantees

A small number of schemes aim to provide guarantees of a particular behaviour. This is often a secondary objective towards increasing consumer confidence or trust. BuySAFE provides a shopper with guarantees of the security of online transactions and identity theft protection insurance. Comodo offers a website identity assurance warranty.

To increase market transparency

This is the stated objective of the EuroPriSe scheme as part of a broader objective of increasing the market for privacy enhancing technologies and practices. This suggests an intention to influence the online environment beyond the relationship between individual users and a website. Gigya states that one of its objectives is to increase transparency between websites and their users.

To resolve disputes

The Confianza Online, buySAFE and the BBB Accredited Business Seal schemes all state that one objective of their seal scheme is to provide dispute resolution mechanisms between websites and website users. The dispute resolution mechanism is intended to give consumers an avenue of response for inappropriate conduct.

6.3.10 Descriptive summary of the schemes and unique selling points

Descriptive summaries of the individual schemes are available in Annex I – Individual seal profiles. As various schemes tend to cluster around a set of ideal types, the models of how the schemes operate are detailed in section 7 – Main convergences and differences.

6.3.11 Privacy and data protection elements of the schemes

A small number of schemes actually appear to have no data protection or privacy elements. This either means that they should not primarily be considered as privacy seal schemes (and are perhaps general trust marks or e-commerce seals as detailed above) or that they have not provided adequate publicly accessible information about the privacy and data protection requirements in the scheme.

Some schemes provide no detailed information on privacy and data protection. For example, Gigya's certification scheme states that it requires data protection for social network information, but does not detail this. Trustify-me requires that a certified site have a privacy policy that "addresses" privacy issues, but the ways in which this should be done are left ambiguous.

Other schemes are focused upon information security rather than privacy and data protection more broadly. Whilst adequate information security is an important component of data protection, these schemes do not make requirements of the other information handling processes of certified organisations. Examples include the McAfee scheme and Verified by Visa. Article 17 of Directive 95/46/EC requires that data controllers must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

Though this is to have regard for the state of the art and the cost of implementing these measures, appropriate measures are to ensure a level of security appropriate to the risks represented by the processing of the data to be protected. Having a contractual agreement with a security provider does not necessarily mean that appropriate security measures to satisfy Article 17 (or its various national transpositions) have been taken (the level of risk could be higher than that protected against by the security provider) but it may be a strong contributing factor towards compliance.

Some schemes draw their privacy and data protection elements from the legal standards with which they are aligned and demonstrate compliance, or from the jurisdiction within which the seal is located (CNIL label, ePrivacyseal, Euro-Label, EuroPriSe, PRIVO, Trusted Shops). Many of these types of schemes are located in the European Union.

Finally, there are schemes that provide detailed privacy and data protection elements, broken down by areas. These schemes often have a code of conduct or best practice criteria that build upon data protection and privacy law, but potentially surpass it. These schemes typically reference security, access, transparency, control over personal data, use and retention, accuracy, disclosure, transfer to third parties and other data protection principles (ESRB, WebTrust, TÜViT Trusted Site Privacy, TRUSTe).

6.3.12 Guarantees offered to data subjects

Many seals do not make specific guarantees to the data subject, including seals that explicitly specify that they do not do so, and do not provide any form of guarantee or warranty regarding personal data (Verified by Visa, Trustify-me, McAfee).

Several seals do not give any additional guarantees to the data subject beyond their already existing legal rights, but do state that the seal indicates compliance with appropriate national or European law (Comodo, CNIL label and TÜViT Trusted Site Privacy Certification). Where guarantees are explicitly directed at the data subject, there are three broad levels of detail. The most abstract level includes seals that largely restate their objectives and discuss the “safety of personal information” (Transaction Guard), “respect for privacy” (BBB Accredited Business Seal) and that “appropriate protective measures have been adopted” (PrivacyMark System).

A greater level of detail is provided by Danish e-mark, Gigya, Fair Data, TRUSTe and Trusted Shops. These schemes break down privacy and security into a number of areas, making more specific guarantees about notice, choice, limited collection, consent, transparency of the use of personal information, accurate privacy policies. To these data protection principles, Gigya offers a range of guarantees associated with information use by social networks and social advertisers.

The third level of granularity is the identification of specific legal guarantees and rights. EuroPriSe provides the largest number of guarantees to the data subject, including transparency, a legal basis for the processing of personal data, including sensitive personal data, compliance with General Data Protection principles and duties, technical-organisational measures and accompanying measures for protection of the data subject. It also guarantees rights under the Directive 95/46/EC (right to be informed, right of access, right of rectification, right of erasure, right of blocking, right of objection to processing) and under the Directive 2002/58/EC (right to be informed of personal data breaches, right to be informed of security risks, right to confidentiality of communications, right to receive non-itemised bills,

right to prevent calling line and/or connected line identification and call forwarding, special rights regarding directories of subscribers to electronic communications services).

buySAFE is unusual in that it offers the data subject live identity theft restoration service and \$10,000 reimbursement for 30 days following the guaranteed transaction. Trustify-me claims to offer a privacy dispute resolution service, but provides no information or contact details for this.

6.3.13 Duration, scope and steps in the certification process

The details of the specific certification processes can be found in Annex I. The study team analysed the certification processes and identified a number of variables. The vast majority of certification schemes follow a typical model as set out below. Significant divergences from this model are also identified.

Stage 1 – Initial application

Typically the entity wishing to become certified initiates the process of obtaining a privacy seal, either through an initial approach to the certification authority expressing interest or by submitting a full application pack or form (either online or by post). Application forms typically require disclosure of relevant aspects of the entity's practices. Seal schemes that rely upon a regulatory standard often ask applicants to demonstrate how they meet this standard. Prices and costs are often negotiated at this stage. This stage may also involve negotiation on what exactly is to be certified or evaluated (for instance, the TÜViT Trusted Site Privacy Certification).

Stage 2 – Assessment

This stage displays the most diversity as different schemes have varying standards and methods for their assessment. One of the key differences is between certification schemes that conduct their assessment purely upon the documentation provided by the applicant, and those that conduct their own investigation (either in-house or using another independent body).

There are three main assessment models identifiable:

- Standard verification. The majority of seal schemes check the applicant's processes for compliance with their programme requirements, codes of conduct, regulatory standards or law.
- Policy consultants. Some seals work with the applicant to develop an appropriate set of data protection policies and practices, and then certify that this has been conducted to an appropriate standard (Trustify-me).
- Service providers provide an additional service or guarantee, and the seal certifies that this service is being provided or is available to the customer (McAfee Secure, buySAFE).

The BBB Accredited Business Seal scheme uses a review board of local businesses. The ePrivacyseal conducts additional optional checks against other standards if the applicant desires. Visa and McAfee rely primarily upon technological tests for functioning software.

Stage 3 – Decision

In this stage, the certification authority makes its decision to award the applicant a seal or not. Several seals allow for the certified entity to make appropriate changes before the final

decision is made. Generally, this stage decision is communicated only to the applicant; however, EuroPriSe makes a shorter version of their decision public.

Stage 4 – Award of seal

Following a successful application and signing an agreement or contract, applicants are generally awarded the right to use the seal. This process is often fairly rapid, sometimes taking as little as one day. The certified entity is often given the HTML code required to display the seal and, if appropriate, is added to public registries maintained by the certification authority.⁶⁶

Stage 5 – Follow-on activity

Not all schemes appear to conduct any regular follow-up activity (i.e., audits) until the renewal process. Some schemes state that they will conduct periodic investigations to check for any deviation from programme requirements or standards. MRS Fair Data requires an independent audit within the first year of certification. EuroPriSe conducts monitoring at eight and 16 months.

There is very little information available on the duration of the certification process. Where information is available, the duration can range from one day (McAfee Secure) to five months (BBB Accredited Business Seal). The duration seems to be primarily determined by the methods and practices of the certification authority.

Stage 6 – Revocation

A final stage may be necessary if the conditions for the revocation of the issued seal are met. This may occur only in the case of a complaint or failed audit, or may occur automatically after a set period of time if there is no re-application.

6.3.14 Coverage of international transfers

The majority of schemes analysed make no specific mention of the international transfer of personal information, and do not identify this as part of their programme requirements. This is likely due to the dominance of schemes based in the United States. BBB does, however, operate a separate EU Safe Harbour privacy dispute resolution programme. European-based seals are much more likely to address international transfers, often in relation to national or European data protection law. MRS Fair Data makes direct reference to the UK Data Protection Act 1998, CNIL to Articles 22, 30 and 31, and Chapter XII of the Loi Informatique et Libertés, and Trusted Shops to EU legal requirements. Confianza online and EuroPriSe refer to their own standards (Article 28 of the Confianza Ethical Code, and sub-set 2.4.2 of the EuroPriSe criteria respectively), although EuroPriSe is based upon European data protection and privacy law.

6.3.15 Costs

⁶⁶ For example, http://www.privo.com/kids_sites.htm or <http://www.trustedshops.co.uk/finder>

The costs are universally carried by the applicant for seal. Many schemes (e.g., buySAFE, Confianza, Seriedad Online) are based upon the total revenue of the application. Others have variable costs based upon the complexity of the audit process, primarily determined by the number of employees (e-mark), or the complexity of the system to be audited (TÜViT Trusted Site Privacy Certification). Discounts are often available for certifying a larger number of websites, paying annually rather than monthly, or taking out a longer term contract. Several charge an initial assessment fee (sometime payable even if the assessment fails) and retest fees (MRS Fair Data), and then reduced costs for renewal. Several seals provided no public information on costs, or suggested that costs may be negotiable. The most expensive seal was Social Privacy from Gigya. CSA is currently free.

6.3.16 Revocation

Many seal schemes do not provide information on the reasons and method for the revocation of their seal. This may make it difficult for consumers or citizens to understand the situation in which a seal should be considered valid. Revocation conditions should be understood alongside the programme requirements of any seal scheme. Where reasons for revocation are given, the most common reason is breaking the terms of the agreement or programme criteria. Other reasons are featured in the following table:

Stated reasons for revocation	Seals
Complaints	buySAFE, Comodo, MRS Fair Data,
Failure to allow access or inspection	buySAFE, TRUSTe
Violation of terms of agreement	BBB Accredited Business Seal, CNIL label, e-mark, PrivacyMark, TRUSTe, Trusted Shops, WebTrust
New, relevant information emerges	TÜViT Trusted Site Privacy Certification, WebTrust
Failure to properly display seal	buySAFE
Violation of any law on the part of the certified entity (as determined by the seal authority)	CSA
Outdated information	CSA
Failure to correct issues raised by seal authority	ESRB, McAfee Secure, PRIVO, Trusted Shops
Failure of annual audit	MRS Fair Data
Violation of own privacy policy	PRIVO, TRUSTe
For any reason	Trustify-me

Table 11: Grounds of revocation

Revocation generally involves the removal of the seal from the offending website or the removal of the right of the website to use that seal, depending upon the appropriate hosting model. Two seals, Verified by Visa and ESRB, indicate that they will fine violations of terms, rather than revoke the seal. Again, this may be troubling in that it does not provide information to the public. Of the schemes that provided information on their revocation conditions, most also had some form of appeal process or allowed the scheme member some time to correct any issues or violations. This ranged from 20 business days for TRUSTe to six months for CSA. The CNIL label and Danish e-mark both allowed one month. McAfee will remove a seal from a website after it continues to fail the technical vulnerability scan for 72 hours.

6.3.17 Recognition

Different seals were recognised in different ways. These forms of recognition are related to the business model or underpinning legal framework of the seal scheme, but also to the way that scheme attempts to promote itself to potential members and other beneficiaries. It was not possible with the data acquired during this analysis to construct a full comparative analysis of the recognition of different schemes within these different categories.

Market recognition

Several schemes attempt to demonstrate their success through the level of market penetration or market share. Verified by Visa is the most significant example of this, whilst TRUSTe highlights its presence on 40 per cent of what it describes as the most trafficked websites.

Public recognition

Public recognition is the extent to which a seal is recognised (and arguably, the extent to which it is seen as meaningful and useful) by the public. The extent of this recognition is generally assessed through consumer surveys, often conducted by the seal schemes themselves, or through external comparative analysis. For example, TRUSTe's own consumer survey suggests that it has high recognition among customer groups,⁶⁷ whilst Comodo's privacy seal scored the lowest consumer recognition in a comparative analysis of a group of privacy seals.

Mutual recognition and partnerships

In this form of recognition, two distinct privacy seal schemes recognise that they will accept the certifications of the other as also meeting their own standards. The PrivacyMark System has a mutual recognition agreement with the Chinese Dalian Software Industry Association. According to a press release, "An entity given PIPA Mark or PrivacyMark accreditation may use 'Mutual Recognition Mark' in their businesses based on the agreement as completed verification of the same requirement level between the standard of PIPA Mark, *Personal Information Protection Regulation for Dalian Software and Information Service Industry* and that of PrivacyMark, *JIS Q 15001:2006 Personal information protection management systems – Requirements* and the demonstration of equivalent procedures for accreditation, resulting in the conformity of the mark systems".⁶⁸

Standards and laws vary between partners, meaning that particular standards of privacy protection may vary dependent upon local law. The two schemes are working to supervise markets in both countries.⁶⁹ The PrivacyMark system also has a mutual recognition programme with the Korea Association of Information and Telecommunication (KAIT).⁷⁰

⁶⁷ TRUSTe, "Customers choose to do business with companies they trust". <http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-websites>

⁶⁸ Japan Information Processing Development Corporation, "DISA and JIPDEC launch mutual recognition program", 30 June 2008. <http://privacymark.org/news/2008/0630/DAIREN20080630.pdf>

⁶⁹ Japan Information Processing Development Corporation, "DISA and JIPDEC launch mutual recognition program", 30 June 2008. <http://privacymark.org/news/2008/0630/DAIREN20080630.pdf>

⁷⁰ Japan Information Processing Development Corporation, "PrivacyMark System," 31 October 2009. <http://privacymark.org/news/2009/1201/ThePrivacyMarkSystem.pdf>

Euro-Label can be understood as a form of mutual recognition too. An example of a partnership is the association between Trusted Shops and the European E-Commerce and Mail Order Trade Association.

Recognition by other seal schemes

This is different from mutual recognition, because in this form of recognition, one seal uses another seal scheme on its own website (presumably having met the established criteria of the second seal). Given that seals offer different guarantees and propositions, this can serve to establish a broader level of confidence at the risk of appearing redundant, and is generally a better practice than self- or auto-certification. BuySAFE primarily offers guarantees on e-commerce, but its website carries TRUSTe certification (for its privacy policy) and the BBB Accredited Business Seal (for its business practices). Comodo is a certified agent for the distributed WebTrust scheme. This cross-certification is not common for schemes with strongly overlapping (and therefore competing) models.

Recognition of seal provider for other services

In several cases, a seal provider has been recognised for other products or services that the company or not-for-profit organisation provides, but not specifically for the privacy seal. For example, McAfee has won several security industry awards, but not for the McAfee SECURE service, whilst the Smart Grid Privacy Seal is a relatively new offering from the company. Similarly, Comodo is a recognised security company, but its privacy seal has comparatively poor recognition.

Recognition by public authorities

Both the ESRB Children’s privacy seal and PRIVO are certified by the US Federal Trade Commission as meeting the requirements for Safe Harbor under the Children’s Online Privacy Protection Act (COPPA). EuroPriSe notes positive receptions from the European Data Protection Supervisor (EDPS) and from the European Commission’s Directorate General for Information Society and Media (now called the Directorate General for Communications Networks, Content and Technology or “DG CONNECT”).⁷¹

Expert recognition

Expert recognition means that a seal scheme or its criteria are recognised by expert groups. This recognition may be post-facto or, as in the case of TÜViT Trusted Site Privacy Certification, a significant expert group may be involved in the development of the criteria and granting recognition from the start.

⁷¹ Reding, Viviane, “Welcome Address,” 14 July 2008. <https://www.european-privacy-seal.eu/events/presentation-of-first-europrise-seal/welcome-address/?searchterm=%20Information%20Society%20and%20Media>

6.3.18 Accredited experts, evaluation bodies and certified experts

The majority of schemes analysed did not accredit external experts or evaluation bodies, with a small number of exceptions. The Better Business Bureau has 113 independent, local BBB organisations which can award the BBB Accredited Business Seal. The CNIL scheme authorises officers to conduct on-site inspections based upon Article 19 of the Loi Informatique et Libertés. MRS Fair Data makes use of an audit partner (Audit Bureau of Circulations) in the UK, and must approve and potentially train any organisations that wish to undertake Fair Data audits, but does not yet appear to have done so. McAfee makes use of a partnership and reseller model for McAfee SECURE, allowing these partners to sell the service, whilst McAfee continues to manage the vulnerability scans. Partners can include e-commerce design and platform providers, hosting companies, payment gateways and strategic partners who could package McAfee SECURE as part of their various services. The PrivacyMark System has 18 assessment bodies. WebTrust is almost entirely administered through accredited experts, as it can be obtained from registered Chartered Accountants and Chartered Public Accountants.

6.3.19 Regulatory and compliance standards

The following table summarises the regulatory and other compliance standards that form the basis of the analysed schemes:

Scheme	Regulatory and other compliance standards
BBB Accredited Business Seal	BBB Code of Business Practices (BBB Accreditation Standards), federal, state and local advertising laws, industry standards
buySAFE	US law, and specifically that of the state of Virginia.
Cloud Security Alliance	Cloud Controls Matrix, or Consensus Assessments Initiative
CNIL label	CNIL standards for labelling products and procedures based on the Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended). Délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés (chapitre V, section 2). The requirements are outlined in the “referentiel” which is published for each procedure or product.
Comodo	Comodo Certification Practice Statement ⁷² ; TrustLogo Subscriber Agreement ⁷³
Confianza Online	Confianza Ethical Code ⁷⁴
Danish e-Mark	-
ePrivacy Seal	EU/German law /IAB Online Behavioural Advertising (OBA) Framework
ESRB	ESRB Principles and Guidelines ⁷⁵ ; Children’s Online Privacy Protection Rule ⁷⁶ (16 C.F.R. Part 312); EU Data Protection Directive (95/46/EC) and

⁷² Comodo, *Comodo Certification Practice Statement*, Manchester, 1 July 2012.

http://www.comodo.com/repository/Comodo_CA_CPS_4.0.pdf

⁷³ Comodo, *Premium subscriber agreement*, 16 July 2002.

http://www.comodo.com/repository/docs/idaauthority_premium_subscriber_agreement.php

⁷⁴ Confianza Online, *Codigo etico de confianza online*, 2011. https://www.confianzaonline.es/documentos-confianzaonline/Codigo_CONFIANZA_ONLINE_2012.pdf

⁷⁵ ESRB, *ESRB Privacy Online: Principles and guidelines*, undated.

http://www.ftc.gov/privacy/safeharbor/esrbpopg_rev.htm

	cookie law ⁷⁷ ; CAN-SPAM; Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)
Euro-Label	Euro-Label European Code of Conduct ⁷⁸
EuroPriSe	EuroPriSe criteria and requirements, based on European rules on privacy and data protection, contained in particular in Directives 95/46/EC, 2002/58/EC and 2006/24/EC.
Gigya	Gigya's SocialPrivacy™ Certification Program Requirements ⁷⁹ , Data Misuse Resolution Policy ⁸⁰ , Social Network Terms of the SocialPrivacy™ Social Networks ⁸¹ .
MRS Fair Data	MRS's Fair Data principles ⁸² and the MRS Code of Conduct ⁸³ ; Data Protection Act 1998, and other standards schemes such as those of the International Organization for Standardization (ISO), the US Safe Harbor Framework and the Data Seal initiative; MRS Data Protection Guidance Document ⁸⁴ .
McAfee SECURE	Payment Card Industry (PCI) Level 1 security standard ⁸⁵ . Vulnerability scanning is part of certification for Health Insurance Portability and Accountability Act (HIPAA) of 1996, Sarbanes Oxley (SOX) regulation, ISO 17799 (now renumbered ISO 27002), and SAS70 (Statement on Auditing Standard No. 70).
PrivacyMark System	JIS Q 15001:2006 (Japanese Industrial Standard for Personal Information Protection Management Systems - Requirements) ⁸⁶ .
PRIVO	The US Children's Online Privacy Protection Act of 1999.
Seriedad Online	Spanish Data Protection Act (LOPD) and the Ley de Servicios de la Sociedad de Información de España (LSSICE).
Smart Grid Privacy Seal	Future of Privacy Forum (FPF) smart grid privacy guidelines and TRUSTe's program requirements for smart grid. The FPF privacy guidelines were developed with reference to the US Federal Trade Commission (FTC)'s Fair Information Practice Principles, the 1980 OECD Privacy Guidelines, North American Energy Standards Board recommended standards for Third-Party Access to Smart Meter-based information, and the California Public Utilities Commission rules regarding privacy and security.
Transaction Guard	None
TRUSTe	TRUSTe Privacy Program Requirements ⁸⁷ .
Trusted Shops	Trusted Shops General Membership Conditions ⁸⁸ ; the ISIS/TS (Internet

⁷⁶ Federal Trade Commission, Children's Online Privacy Protection Rule, Final rule, Federal Register, Vol.78, No.12. 17 January 2013. <http://www.ftc.gov/os/fedreg/2013/01/130117coppa.pdf>

⁷⁷ European Parliament and Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 24 October 1995. http://europa.eu/legislation_summaries/information_society/data_protection/114012_en.htm

⁷⁸ Euro-Label, *The European Code of Conduct*. <http://www.euro-label.com/en/code-of-conduct/index.html#c217>

⁷⁹ Gigya, *Program Requirements*, 24 January 2013. <http://www.gigya.com/solutions/social-privacy/program-requirements/>

⁸⁰ Gigya, *Misuse Resolution*, 2013. <http://www.gigya.com/solutions/social-privacy/misuse-resolution/>

⁸¹ Gigya, *Social Network TOS*, 13 December 2012. <http://www.gigya.com/solutions/social-privacy/program-requirements/sn-tos-principles/>

⁸² Fair Data, *Ten Principles*, 2013. <http://www.fairdata.org.uk/10-principles/>

⁸³ Market Research Society, *Code of Conduct*, April 2010.

⁸⁴ Market Research Society, *The Data Protection Act 1998 & Market Research: Guidance for MRS Members*. September 2003.

<https://www.mrs.org.uk/pdf/The%20Data%20Protection%20Act%201998%20and%20Market%20Research.pdf>

⁸⁵ Payment Card Industry, *PCI Data Security Standard: Requirements and security assessment procedures. Version 2.0*. October 2012. https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

⁸⁶ <http://webstore.ansi.org/RecordDetail.aspx?sku=JIS+Q+15001%3a2006>

⁸⁷ TRUSTe, *TRUSTe Program Requirements*, Undated. <http://www.truste.com/privacy-program-requirements/>

	Shopping is Safe / Trusted Shops) Code of Practice ⁸⁹ ; criteria based on consumer protection requirements as well as national and European legislation
Trustify-me	None
TÜViT Trusted Site Privacy Certification	Trusted Site Privacy criteria ⁹⁰
Verified by Visa	Acquirer and Merchant Implementation guide; Visa Operating Regulations; Cardholder Information Security Plan; Payment Card Industry Data Security Standards.
WebTrust	WebTrust principles and related criteria ⁹¹ developed by the AICPA and the CICA, specifically the Generally Accepted Privacy Principles (GAPP). ⁹²

Table 12: Regulatory and compliance standards

6.3.20 Frequency and means of updates to schemes

The study team found little information on the frequency and means of updates to the schemes. Whilst some schemes do appear to change over time (McAfee SECURE was previously McAfee HackerSafe, and was originally acquired by the company during a corporate takeover. WebTrust's terms of service were updated in August 2009, and Verified by Visa is trialling new technology), these seem to be driven by business reasons rather than on a regular timescale. It is difficult to determine if the other schemes are consistent over time, or if they change their programme requirements but do not keep a public record of these changes.

The most detailed information of frequency and means of updates to the scheme come from CNIL, EuroPriSe and PrivacyMark. If CNIL changes its standards, old seals remain valid, but must meet the new standard for their next renewal (which could be up to three years). EuroPriSe is based upon European Directives on privacy and data protection, and is applied in line with the EU law and the opinions issued by the Article 29 Data Protection Working Party. It was amended in 2010 in response to Directive 2002/58/EC (Directive on privacy and electronic communications). The PrivacyMark System is subject to periodic review by the Japan Information Processing (JIPDEC) secretariat, whilst an assessment body meets every two weeks to discuss any operational issues. JIPDEC also commissions an annual public survey to highlight any issues and takes remedial action accordingly. McAfee SECURE updates its vulnerability database daily, but again provides no information on changes to its programme requirements.

⁸⁸ Trusted Shops, *Trusted Shops Membership Terms*, 02 April 2013.

http://www.trustedshops.co.uk/tsdocument/TS_PRIME_TIME_TERMS_en.pdf%E2%80%8E

⁸⁹ Trusted Shops, *Code of Practice*. 25 July 2013.

http://www.trustedshops.com/tsdocument/TS_QUALITY_CRITERIA_en.pdf

⁹⁰ TÜViT, *Trusted Site Privacy: Proof of Privacy Conformity*. <https://www.tuvit.de/en/privacy/trusted-site-privacy-1083.htm>

⁹¹ Canadian Institute of Chartered Accountants, *Trust Service Principles and Criteria for Certification Authorities. Version 2.0*. March 2011. <http://www.cica.ca/resources-and-member-benefits/growing-your-firm/trust-services/item10797.pdf>

⁹² Canadian Institute of Chartered Accountants, *Generally Accepted Privacy Principles*.

<http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/gen-accepted-privacy-principles/item10717.aspx>

6.3.21 Additional elements

Additional elements are available in the individual profiles in Annex I.

6.3.22 Complaints mechanisms

There are four main types of complaint mechanisms identifiable in relation to the analysed seals: No complaints mechanism, an e-mail address or web form, complaint about a member to the certification authority, and complaint to the member directly, with the certification authority as last recourse.

Several schemes provide a contact e-mail address for complaints, without providing information about the process or what a complainant might expect from this process (buySAFE, CSA, EuroPriSe, McAfee Secure, Trustify-me, Verified by Visa). BBB Accredited Business Seal, Comodo, Confianza, PrivacyMark, PRIVO and Seriedad Online will accept complaints from individuals and then pass these on to their members. ESRB, Gigya, MRS Fair Data, Smart Grid Privacy and TRUSTe ask complainants to contact the member company directly, with these companies acting as a dispute resolution service if there is no response or the response is unsatisfactory to the complainant. PRIVO, Trusted Shops and TÜViT Trusted Site Privacy Certification require members to have a functional complaints process.

Most of the schemes do not mention a cost for making a complaint, whilst several do mention that the process is free. The two exceptions are Trusted Shops, which may levy a fee upon a member as part of an upheld complaint, and WebTrust, where the losing party in a complaint pays the costs of arbitration, which can range from \$49 to \$150 depending upon complexity.

Most of the schemes allow complaints from any member of the public. Seriedad Online and Confianza both allow complainants to make complaints about businesses that are not scheme members. In these cases, these seals will attempt dispute mediation.

6.3.23 Criticisms

The following table summarises common criticisms of the analysed seal schemes. These criticisms combine those identified during the literature (including media) review and issues and problems identified by the partners during the research process.

Criticism	Schemes
Too close relationship with scheme members	BBB Accredited Business Seal ⁹³ ,
Relationship with scheme members driven by commercial profit	BBB Accredited Business Seal ⁹⁴ , McAfee
Bias towards accredited business members	BBB Accredited Business Seal ⁹⁵ , McAfee ⁹⁶
Disregards complaints	BBB Accredited Business Seal ⁹⁷

⁹³ Rhee, Joseph and Brian Ross, "Terror group gets 'A' rating from Better Business Bureau", *ABC News*, 12 Nov 2010. <http://abcnews.go.com/Blotter/business-bureau-best-ratings-money-buy/story?id=12123843>

⁹⁴ Rhee, Joseph and Brian Ross, "Terror group gets 'A' rating from Better Business Bureau", *ABC News*, 12 Nov 2010. <http://abcnews.go.com/Blotter/business-bureau-best-ratings-money-buy/story?id=12123843>

⁹⁵ Ibid.

⁹⁶ <http://siteadvisor-complaints.com/>

Complaints registered with authorities	buySafe ⁹⁸
False seals in circulation/use	CNIL label ⁹⁹ , PrivacyMark, TRUSTe ¹⁰⁰ , Verified by Visa ¹⁰¹
Security flaws	Comodo ¹⁰² , McAfee ¹⁰³ , Verified by Visa ¹⁰⁴
Inefficient process	Confianza ¹⁰⁵
Weak or vague guarantees	ESRB, Gigya
Inactive elements, out-of-date websites	Euro-label, PRIVO ¹⁰⁶ , Smart Grid Privacy Seal
Lack of interest and low take-up	Euro-Label ¹⁰⁷ , EuroPriSe
Poorly accessible policy details	Gigya, MRS Fair Data, PRIVO, Smart Grid Privacy Seal, Transaction Guard, Trusted Shops, Trustify-me
Contact details poorly accessible	Trustify-me
Charges, cost structure	McAfee, Verified by Visa ¹⁰⁸
Blurring between overlapping schemes	McAfee, PRIVO, Trustify-me
None found	CSA, e-Mark, ePrivacyseal, Seriedad, TÜViT Trusted Site Privacy Certification

Table 13: Criticisms

Too close a relationship between a seal scheme and members might suggest that they are drawn from the same community or area of business and that the scheme is not independent. Although many schemes are for-profit business models, this becomes a criticism if the pursuit of profit is seen as overwhelming the purposes and objectives of the scheme. A bias towards members can be found if a seal scheme provides some kind of listing or search function. For example, McAfee's Site Advisor plug-in for web browsers highlights McAfee SECURE clients in search results. If false or illegal uses of the seals have been identified, then this can reduce confidence in the seal scheme. Security researchers have identified security flaws in

⁹⁷ Rhee, Joseph and Brian Ross, "Terror group gets 'A' rating from Better Business Bureau", *ABC News*, 12 Nov 2010. <http://abcnews.go.com/Blotter/business-bureau-best-ratings-money-buy/story?id=12123843>

⁹⁸ BBB, Business Review: Buy Safe Inc, <http://www.bbb.org/washington-dc-eastern-pa/business-reviews/internet-services/buy-safe-inc-in-arlington-va-7004236/>

⁹⁹ Winston & Strawn LLP, "Biometrics: French officials warning", *Briefing*, February 2007.

¹⁰⁰ Edelman, Benjamin, "Coupons.com and TRUSTe: Lots of Talk, Too Little Action", 18 March 2008. <http://www.benedelman.org/news/031808-1.html>

¹⁰¹ Brignall, Miles, "Verified by Visa Scheme confuses thousands of internet shoppers", *The Guardian*, 21 April 2007. <http://www.guardian.co.uk/money/2007/apr/21/creditcards.debt>

¹⁰² Zetter, Kim, "Hack obtains 9 bogus certificates for prominent websites; traced to Iran", *Wired: Threat Level*, 23 March 2011. <http://www.wired.com/threatlevel/2011/03/comodo-compromise/>

¹⁰³ Goodin, Dan, "McAfee, Trust Guard certifications can make websites less safe", *ARS Technica*, 6 Oct 2012. <http://arstechnica.com/security/2012/10/mcafee-trust-guard-certifications-can-make-websites-less-safe/>

¹⁰⁴ Murdoch, Steven J. & Ross Anderson, "Verified by Visa and Mastercard SecureCode: Or, How Not to - Design Authentication", in R. Sion (ed), *Financial Cryptography and Data Security*, LNCS 6052, 2010, pp. 336–342; Ferguson, Rik, "Verified by Visa?", *Countermeasures*, 01 Dec 2011. <http://countermeasures.trendmicro.eu/verified-by-visa/>

¹⁰⁵ http://www.ciao.es/Opiniones/confianzaonline.org_404068

¹⁰⁶ Connolly, Chris, *Privacy White Lists: Don't be Fooled*. Galexia, 2009. http://www.galexia.com/public/research/assets/privacy_white_lists_2009/

¹⁰⁷ Databank Consulting. *Case Study: Euro-label*. Milan, 2004. http://ec.europa.eu/enterprise/archives/e-business-watch/studies/case_studies/documents/Case%20Studies%202004/CS_SR06_Retail_2-Euro-Label.pdf

¹⁰⁸ Murdoch, Steven J. & Ross Anderson, "Verified by Visa and Mastercard SecureCode: Or, How Not to - Design Authentication", in R. Sion (ed), *Financial Cryptography and Data Security*, LNCS 6052, 2010, pp. 336–342.

seal schemes, which range from exploitable vulnerabilities to a failure to identify other security flaws.

Verified by Visa has been criticised for encouraging insecure behaviour (entering additional personal information and payment card details into an unexpected pop-up window). Some of the smaller seal schemes appear to have a lack of interest from potential members based upon their applicability (the population of potentially eligible entities) and their current number of members. Out-of-date or missing information on a scheme undermines the scheme as users cannot easily find information upon which to base their decisions. Blurring between different schemes occurs when a seal provider has a range of privacy and security products or solutions, and it can be difficult to distinguish what each of them covers. Many of these criticisms relate to the lack of accessibility of information on the scheme and the way that this information can be verified.

6.3.24 Links and references to schemes

Links and references to the schemes are available in the individual profiles in Annex I.

6.3.25 Logos

Given that privacy seals tend to be viewed rapidly and non-specifically, more frequently than they are interrogated in detail, the appearance is likely to be quite important. The appearance of privacy seals is an area where there is substantial convergence.



Figure 2: Scheme logos

Part of the function of a privacy seal image is, understandably, resembling a privacy seal or, at the very least, resembling what a user might expect a privacy seal to look like. However, as part of a branding exercise, each privacy seal attempts to distinguish itself from others, and stand out against other alternative schemes. Therefore, we might anticipate that later privacy seals draw design inspiration from earlier privacy seals, whilst exhibiting some variation. The goal would be a seal design that is recognisable as a privacy seal, but also distinctive enough to develop its own recognition factor. The exception to this pattern will be scam or fraudulent privacy seals¹⁰⁹, which will attempt to copy this visual grammar in order to deceive a visitor to the website.

Another visual design constraint on the privacy seal is anticipation of the contexts into which they will be placed. The inception of privacy seals over time also demonstrates a shift with common online design styles (see section 6.3.3). Contrast 2012's Gigya SocialPrivacy seal with 1999's ESRB seal. Seal providers appear to go to some effort to guarantee the consistent representation of their privacy seals. A common element of many terms of use is an agreement not to alter or modify the appearance of the privacy seal, or stipulations on the placement and location of the seal. Some schemes (including McAfee) make alteration of the seal impossible, by serving the seal image from their own servers.

The seals generally display in a similar size. For seals with a discernible edge against a white background, a rectangle with rounded corners is the most common shape. Again this is likely a feature of contemporary web design trends.

The most common main colour for a privacy seal is blue. Yellow is the second most common colour and a frequently used accent colour. Blue has a number of common colour connotations and associations which privacy seals might be seeking to exploit, including reliability, stability, security, calmness, reflection, cleanliness, intellect, precision, authority. It is a common corporate colour. Yellow has associations with energy, intellect and is used in design to attract attention. Blue and yellow contrast well together, so their association is not surprising. Privacy seals often use white in their design, either as a background for blue or black text (BBB Accredited Business Seal, PrivacyMark, Gigya, Verified by Visa, Trusted shops, McAfee Secure, TRUSTe, Privacy Seal, EuroPriSe, Smart Grid Privacy seal and Fair Data) or for white text on a blue background (CNIL label, PRIVO, WebTrust, CSA, ESRB). Seals often feature white space around the seal, which likely helps integration with a range of websites, where white backgrounds predominate. White has associations with purity, safety and cleanliness, and simplicity. Black is the third most common colour for text in the seals analysed. Black has associations with formality, strength and authority; it is a high contrast colour, increasing the legibility of the text.

McAfee SECURE, Comodo and TRUSTe stand out somewhat from the other seals through their use of alternate colours, red and green respectively.

Given the limited colour palette in use, one of the key elements of variation in the privacy seals are the logos themselves, but even here the iconography is relatively constrained. Some utilise iconography, which includes torches (BBB Accredited Business Seal), stylised silhouettes (PrivacyMark, Gigya's SocialPrivacy), globes (WebTrust, EuroPriSe, Trustify-me) padlocks (Privo, although the CNIL seal is reminiscent of a padlock in shape), and

¹⁰⁹ Contrasted with sites that are fraudulently using a real seal they are not authorised to use.

oversized instances of the letter “E” (Trusted Shops, TRUSTe). Several seals also build upon a brand identity established elsewhere (Verified by Visa, McAfee).

6.3.26 Websites

Details of the websites for the analysed schemes can be found in the individual analyses in Annex I. Some further notes on the accessibility and information contained on the websites of different seals can be found in section 6.2.1.

6.4 ANALYSIS OF PRIVACY SEAL SCHEMES AGAINST GDPR CRITERIA

The draft GDPR requirements were introduced only in early 2012 and their exact contents and particulars of implementation are still being debated at the highest EU level. As this content is yet to be finalised (if it is assumed that all criteria in the original 2012 draft will make it through the EU law-making process), it is perhaps not appropriate to assess privacy certification schemes that are already operational against the GDPR criteria that will become enforceable in the future – just as it would be unfair to assess the existing data protection legislation of Member States against the same. The following analysis must therefore not be construed as evidence of the failure of (practically all) of the analysed schemes under examination to apply the (novel) GDPR criteria; instead, it would be preferable if this fact-finding exercise and comparative analysis is used to assess the readiness of these schemes to accommodate the GDPR criteria, whenever these are finalised and become binding within the EU.

A number of distinctions need to be made before elaborating upon how well the analysed schemes perform in relation to the GDPR criteria. The first one pertains to the distinction between general and privacy-specific certification schemes. The general schemes analysed (e-commerce trust marks) aim at enhancing consumer confidence, providing reassurance that a certified entity complies with relevant regulations and broadly adopts responsible business practices. Privacy and data protection concerns (for instance, how consumer data is processed) do play a part in such schemes, but they form only a small part of the many parameters of these schemes. In practice, we found that no more than a single article, or at best a section, in the code of conduct of general schemes analysed was devoted to privacy and data protection issues. Though the general schemes aim to deal with privacy and data protection concerns as well as possible, as one might expect, they do not do so to the same extent as privacy-specific schemes. Nevertheless, the co-existence of general trust marks and privacy-specific trust marks, both expressly aiming at creating consumer trust, invites discussion on whether privacy trust marks could be treated as a part of e-commerce regulation (i.e., in the Directive on electronic commerce¹¹⁰) rather than the other way around (general trust marks to be judged against the Data Protection Directive 95/46/EC or GDPR), as is the case today. However, this approach may exclude many processing operations not directly facing consumers, for example, in the e-health sector. This idea shall be elaborated in detail later on in the Study (specifically in Task 4 which focuses on policy options).

¹¹⁰ European Parliament and the Council, Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, Brussels, 17 July 2000, pp. 1-16.

The second distinction relates to EU and non-EU schemes. The origins of the schemes under examination substantially affect the rules and guidelines applicable to its participants: those originating within the EU have to comply with the criteria of their national data protection acts and, consequently, with the criteria of the Data Protection Directive 95/46/EC (this is particularly visible in DPA-sponsored schemes such as the CNIL label or EuroPriSe). On the contrary, schemes based outside the EU have to either develop their own data protection policies based on the data protection practices in the relevant jurisdiction (as is the case with the USA-originating schemes) or comply with their national privacy or data protection provisions, whatever these may be. Although the GDPR will be applicable to websites targeting EU individuals, evidently, non-EU privacy seal schemes are not expected to fare well with the GDPR criteria (and perhaps not even with the provisions of the EU Data Protection Directive), considering that these practically further and deepen the purposes of the Data Protection Directive.

Finally, a third distinction is of a legal nature: a number of the GDPR criteria are also found in the text of the Data Protection Directive. This is, for instance, the case with the fundamental personal data processing principles (for instance, fair and lawful processing, data quality, purpose limitation, etc., as included in Article 6.1 of the Directive) or data controller liability (Article 6.2 of the Directive), where differentiations are noted only at the data protection periphery (for instance, special provisions for the protection of children). On the other hand, the draft GDPR introduces a number of novel data protection provisions, such as the right to be forgotten, right to data portability and data protection impact assessments. This distinction has affected the findings of the analysis that follows: while the multitude of (EU) schemes generally score well when it comes to GDPR criteria that also constitute core Data Protection Directive criteria, this is usually not the case with the GDPR novelties (e.g., the right to be forgotten, the right to data portability, etc.) or additions to older data protection principles (e.g., protection of children, increased documentation obligations, etc.). Some of the new potential elements of the GDPR, such as the right to be forgotten, may be difficult for existing seal schemes to implement.

The following analysis focuses on the main criteria of the draft GDPR, i.e., its principles (items 33-40 in Table 27 collated scheme assessment table, Annex I), the data subject rights (items 41-52 in Table 27), data controller and processor accountability (items 53-60, Table 27) and international data transfers (item 45, in Table 27). The study team found that EU-originating schemes do aim to adhere to the provisions of the Data Protection Directive, but have varied degrees of readiness when it comes to applying the admittedly stricter and more elaborate provisions of the draft GDPR. As far as non-European schemes are concerned, if a general conclusion were at all possible when comparing schemes originating in the different jurisdictions of Japan, Canada and the USA, they are, in the best cases, implementing a privacy policy that includes some, but not all, of the basic EU data protection principles and are currently closer to the Data Protection Directive than the proposed GDPR.

6.4.1 Principles

The basic data protection principles in the GDPR are listed in items 33 to 40 of Table 27. Practically all the items (except item 39) refer to principles that are common to the Data Protection Directive (see Article 6) and the GDPR. The fair and lawful requirement, data quality requirements, purpose limitation, as well as the designation of the data controller as the entity liable for the personal data processing are well established requirements of the Data Protection Directive – these have been repeated, in more or less the same wording, in the draft

GDPR (as outlined before). The only exemption to this rule is item 39 pertaining to parental consent in the event of the processing of personal data of children – this requirement for special care when it comes to handling such personal information is only found in the text of the GDPR.

Given the above, it comes as no surprise that practically all EU-originating schemes analysed in this report score well in relation to the above requirements (items 33 to 40, with the exception of item 39; see, however, *Confianza Online Ethical Code*). While non-profit organisations' schemes (for instance, Euro-Label, *Confianza Online*, Market Research Society (MRS) Fair Data Mark) and particularly DPA-sponsored schemes (such as the CNIL label or EuroPriSe) generally observe the Data Protection Directive provisions closely, results vary when it comes to for-profit organisations (for instance, ePrivacyseal or Seriedad Online or Trusted Shops set high standards¹¹¹, but this is not the case with Comodo Secure). The basic personal data protection principles have been well incorporated into the respective codes of conduct for the schemes concerned; however, only a handful granted special attention to the processing of data referring to children (for instance, the CNIL label, *Confianza Online* or Euro-Label).

On the other hand, the basic personal data processing principles of the EU Data Protection Directive do not constitute in their entirety and exact wording the international standard. Some of them, for instance, provisions on data quality or the liability of the data controller may be found outside the EU as well. The Fair Information Principles found in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data¹¹² provide a useful listing to this end.¹¹³ Nevertheless, non-EU states have not embraced the strict EU approach on such issues as purpose limitation or time-restricted and proportionate personal data processing.

The above clarifications are illustrated also in the text of non-EU schemes analysed in this report. In their majority, such schemes include provisions incorporating more (for instance, TRUSTe, WebTrust, the ESRB Privacy Online Certification, the PrivacyMark System, Smart Grid Privacy Seal) or less (for instance, BBB Accredited Business Seal, buySAFE Guaranteed Shopping, Gigya's SocialPrivacy™ Certification) the Fair Information Principles in a wording that is closer to the OECD Guidelines than the GDPR or the Data Protection Directive. This finding is valid for all items examined here (items 33-40, Table 27), including provisions on special protection measures for children (with the particular exception, regarding the protection of children, of the ESRB Privacy Online Certification and PRIVO Privacy Certified).

6.4.2 Rights of the data subject

Unlike the basic personal data processing principles analysed above, where the GDPR more or less repeats the provisions of the Data Protection Directive and only marginally affects their application particulars, the draft GDPR substantially expands the list of data subject rights. Data subject rights were originally conceived as a special subset of rights (to

¹¹¹ Setting high standards does not rule out that there may be implementation and enforcement issues.

¹¹² Organisation for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980.

¹¹³ See Part Two of the Guidelines, in particular: the collection limitation, data quality, purpose specification, use limitation, security safeguards and accountability principles.

information, access, rectification) that would assist data subjects while exercising their individual right to data protection (given the fact that they are often found at a disadvantage in relation to third party processing of their personal information). The list of the three basic rights was upheld in the draft GDPR, and new ones were added to it, namely the right to be forgotten and the right to data portability. Notwithstanding the continued discussions on their applicability and usefulness to data subjects, these two new rights are listed in items 48 and 49 in Table 27. The remaining items, 41 to 52, more or less refer to the basic rights of information, access and rectification, repeating or expanding, where necessary, the wording of the EU Data Protection Directive in accordance with the draft GDPR (see, for instance, item 44).

Here too, the analysed EU-based schemes scored well when it came to items that more or less reflected data controller obligations and data subject rights respectively, that are already in place under the EU Data Protection Directive (see, in particular, its Articles 10-14). This is particularly the case for items 41, 42, 43, 45, 46, 47, 50 and 52. In all these cases, presumably because they reflect legal obligations imposed on data controllers by the Directive (and, therefore by national data protection acts), practically all EU schemes included relevant provisions in their codes of conduct. Nevertheless, if a finer distinction needs to be made, (as in the case of the preceding analysis of principles), DPA-sponsored schemes (such as the CNIL label or EuroPriSe) along with non-profit organisations' schemes (for instance, Euro-Label, Confianza Online, Market Research Society (MRS) Fair Data Mark) generally observe the Data Protection Directive provisions closely, while results vary when it comes to schemes of for-profit organisations. While ePrivacyseal or Seriedad Online set relatively high standards, this is not the case with Comodo Secure.

None of the analysed schemes include any explicit provisions on the right to be forgotten or on the right to data portability (items 48 and 49 respectively). This is probably to be expected because these matters are still being debated at EU level, and therefore the relevant provisions in the proposed GDPR are yet to be finalised. Also, such measures are generally perceived as not likely to be popular with some organisations, which presumably would not opt voluntarily to subscribe to or implement a scheme that pushes them in this direction without a firm legal obligation to do so.

Finally, a special mention should be made of direct marketing (item 51). Certain schemes analysed had relevant provisions dealing with direct marketing, some of which permit individuals to object free of charge to the processing of their personal data for such purposes (for instance, Euro-Label, Confianza Online, Trusted Shops, TRUSTe, the PrivacyMark System. The DPA-sponsored schemes such as EuroPriSe or CNIL label set the highest standards in the field).

Non-EU schemes perform varyingly with regard to data subject rights, because the EU list is EU-specific and, admittedly, far from constituting the international standard (the OECD Guidelines, for instance, provide relatively little assistance to this end – (see, however, Article 13 on the individual participation principle). Each non-EU organisation that released a certification scheme implements its own privacy policy. Such policy may (for instance, TRUSTe, WebTrust, buySAFE Guaranteed Shopping, ESRB Privacy Online Certification, PrivacyMark System) or may not (for instance, BBB Accredited Business Seal, Gigya's SocialPrivacy™ Certification) protect individuals by granting them a right to information, access and rectification. Protection may occur at varied levels (for instance, the Cloud Security Alliance is very explicit on data breaches and security obligations, as part of a cloud

application, but not as explicit on the rest of data subject rights) and be provided under different circumstances. In this context, generalisations about the analysed non-EU privacy seal schemes are impossible; each ought to be examined on its own merits.

As one might expect, the same is true with regard to the rights to be forgotten and data portability; no reference to them is found in the analysed non-EU schemes.

6.4.3 Controller and processor obligations

Accountability circumstances for data controllers and data processors attracted, and continue to attract, much attention during the GDPR elaboration. A new principle, the principle of accountability, is being discussed as the means to levy the bureaucratic burden imposed on data controllers across the EU by the Data Protection Directive. However, the provisions currently under discussion have been accused of overstressing the limited resources of SMEs (even if there is a level of exemption for SMEs). In any event, even in the wording of the Data Protection Directive, the data controllers (and at times data processors) are liable for the processing they undertake.¹¹⁴ This basic principle (item 38 of Table 27) led to concrete obligations being imposed on, mostly, data controllers. The text of the draft GDPR alters such obligations; the elimination of the notification scheme and the adoption of a principle of accountability have brought forward a series of new obligations, as, partially, depicted in items 53 to 60 of Table 27.

As this is arguably the field that underwent the heaviest restructuring in the draft GDPR, even the EU-originating schemes scored low in the relevant criteria. These schemes take the provisions of the Data Protection Directive for granted and are perhaps hesitant to impose upon their participants any new obligations not prescribed by law; this may be the reason why criteria as documentation requirements, or personal data breach policies or the use of impact assessments (items 53, 55 and 56, 57 respectively of Table 27) are not found in the EU schemes (with the exception of DPA-sponsored schemes such as the CNIL label and EuroPriSe).

Scheme operators generally had no problem demonstrating compliance with existing requirements such as designation of a data protection officer (item 59 of Table 27) or the implementation of data security measures (item 54 of Table 27). However, the application of prior consultation and authorisation procedures (item 58 of Table 27) should not necessarily be interpreted as complying with the provisions of the draft GDPR, but rather with requirements already in effect under the EU Data Protection Directive and resulting Member State data protection acts.

Though the GDPR-based analysis of the schemes did not have a specific category devoted to Article 23 (data protection by design and by default), the study team recognises that privacy seal schemes could be of great value in certifying that specific products or services have been designed in accordance with this principle. None of the schemes analysed seemed to have this explicit requirement.

The principles incorporated in the GDPR (data breach policies, data protection impact assessments) could not be found in relation to non-EU based schemes. Nevertheless, in

¹¹⁴ See Articles 6.2 and 17 of the Directive.

relation to implementing security measures, some of the analysed non-EU schemes were found to be stricter, or at least more explicit, than the EU-based schemes, particularly subject-specific certification schemes. See, for instance, the CSA, the Smart Grid Privacy Seal and Verified by Visa for cloud computing, smart grid systems and credit card payments respectively.

In essence, apart from general consensus and assigning the responsibility and liability of the processing to a single person (the controller, see also Article 14 of the OECD Guidelines), the rest of the relevant items in Table 27 should generally be considered as lacking in non-EU schemes. Notable exceptions are: TRUSTe (data breach notifications) and WebTrust (internal and external oversight).

6.4.4 Transfer of personal data to third countries or international organisations

As the schemes analysed in this report are largely national or regional in scope, few of them aspire to regulate cross-border data flows of their participants. This is particularly true for the EU-based schemes where it is perhaps felt that the provisions of the Data Protection Directive, and the respective national data protection acts, are sufficient. Several EU-based schemes are, directly or indirectly, exclusively single country-oriented (CNIL label, Confianza Online, Danish e-mark). Other schemes, such as the Euro-label scheme, have appointed local representatives at Member State level rather than operating centrally for all Member States (note this scheme is currently functioning only in Austria and Germany). Very few (for instance, the CNIL label, Confianza Online, Market Research Society (MRS) Fair Data Mark) provide guidance on cross-border data flows to their members (item 17 and/or 45(7) of the Table 27).

However, this is not the case with non-EU certification schemes. In USA-based schemes, the issue of cross-border data flows is central in the relevant policies. Some schemes, for instance, the BBB Accredited Business Seal or PRIVO Privacy Certified, adhere to the Safe Harbor policies or implement their own, ad hoc solutions (see, for instance, McAfee SECURE). Others, such as Japan's PrivacyMark System adopt a bilateral approach. Evidently, the issue of international transfers, particularly with EU Member States that are obliged to apply strict data protection rules, is of particular importance to both providers and participants in non-EU privacy seal schemes. This is why in most cases, relevant information, and even policies, are available to scheme participants and users alike.

7 MAIN CONVERGENCES AND DIFFERENCES

This section brings together all the results of the research and analysis of the different privacy certification schemes and presents them in an innovative manner so as to highlight convergences and differences in relation to seal models, objectives of the schemes, EU and non-EU based schemes, compliance and regulatory standards, rights of data subjects, complaints redress and shared problems and the requirements of the GDPR. The section adopts a holistic analysis of the schemes as a whole.

7.1 SEAL ACCESSIBILITY MODELS

We can identify a small number of core models around which the analysed schemes converge. Many operate in broadly similar models, with the differences between them being variables

within those models (for example, two schemes might operate along the same model but have different durations for their certification process or charge different fees). These models are not based upon pre-existing categorisation, but rather from a collective examination of the way that the privacy seals examined in this study appear to work. The primary means of categorisation is the flows of information within the model, the sources of authority and certification, and how the seal is provided to a particular certified entity and thereby made visible to the website user. The structure and process of a given seal is key for understanding the reliability of a seal and its proper implementation.

Model	Short description	Schemes
Classic seal	The most basic seal, in which certification grants the rights to display a seal, including on offline material.	PrivacyMark (offline), BBB Accredited Business Seal (offline) CNIL label
Linked seal	Builds upon the classic seal model by turning the seal itself into a hyperlink to information on the seal scheme, typically hosted on the website of the certification authority	PrivacyMark (online), Danish e-mark, MRS Fair Data
Hosted seal	The seal image is hosted from servers controlled by the certification authority. Typically, the seal also contains a unique link back to the certification authority.	Comodo, Confianza, e-mark, Trustify-me, ESRB, PRIVO, Seriedad, TRUSTe, Smart Grid Privacy Seal
External standard seal	The certification authority has no control over the standard, but has been entrusted to certify third parties against this standard	PRIVO, ePrivacyseal, ESRB, TÜViT Trusted Site Privacy Certification
Delegated certification seals	A large number of independent assessors, with the seal provider playing the role of standard-setting agency.	WebTrust, TÜViT Trusted Site Privacy Certification
Federated seals	Multiple certification authorities agree amongst themselves on a shared standard (often a shared minimum standard).	Euro-Label
Security scan seals	Certified entity is effectively re-certified every day, through a security vulnerability scan conducted by the seal scheme.	McAfee Secure
Insurance seals	Rather than certifying that certain security or data protection measures have been taken, the seal guarantees that if identified problems do arise, then the customer will be insured.	BuySafe
Registry (self-assessment)	Certification authority maintains a register of information on certified entities. This register is accessible to the intended audience of the scheme.	CSA
Registry (investigative)	Scheme compiles its own information on websites or service	None, potentially Gigya Social Privacy.

	providers, and then makes this information publicly available.	
3-D Secure	Transaction security method for online payments	Verified by Visa

Table 14: Model-based classification of schemes

In the following part, seal models are illustrated with diagrams. These depict the key actors in a seal scheme and their relationships with each other. A double-headed arrow represents a negotiated or co-operative process, whilst a single arrow demonstrates a relationship where one party primarily acts upon another, or provides information in a particular direction. The dark blue arrows represent structural arrangements, whilst the lighter arrows depict the information flow from the end-user perspective.

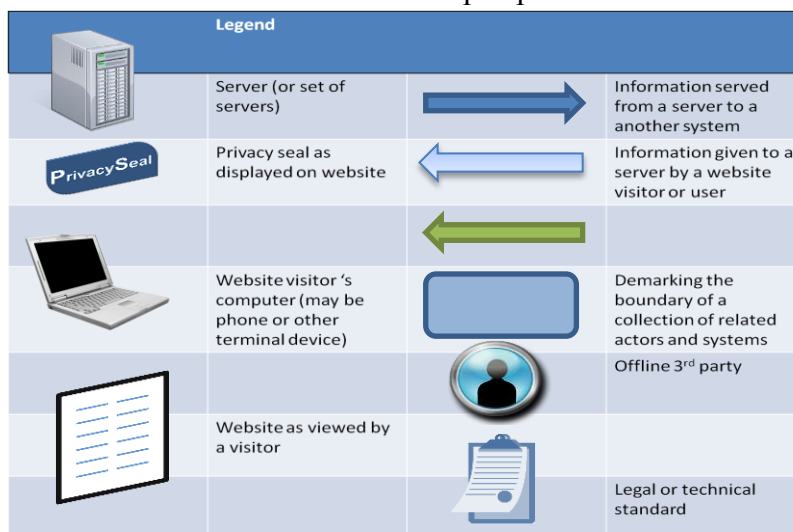


Figure 3: Legends for the seal models

The classic (or minimal) seal

This model is the most basic model for constructing a privacy seal, but it has some inherent flaws. It is the minimum functional requirement for a seal scheme. We provide the model here because many of the subsequent models are actually variations upon it, with the intent of addressing flaws or gaps in this model. This model is also applicable for seals in non-hyperlinked media (for example, on print publications or non-interactive video). In these cases, a user wishing more information on the seal or the certified entity must seek this out manually, although seals in this mode of delivery generally have a web address. Key areas of variation in the classic model include the details of the certification process (see section 6.3.13) and the terms for the provision of a seal (see section 6.3.19).

The classic, linked and hosted seals are really a development of the same model, making an increasingly more specific linkage between the displayed seal, and the certification claims made by the seal provider, as well as reducing the effort that a website visitor has to exert in order to investigate and verify that linkage.

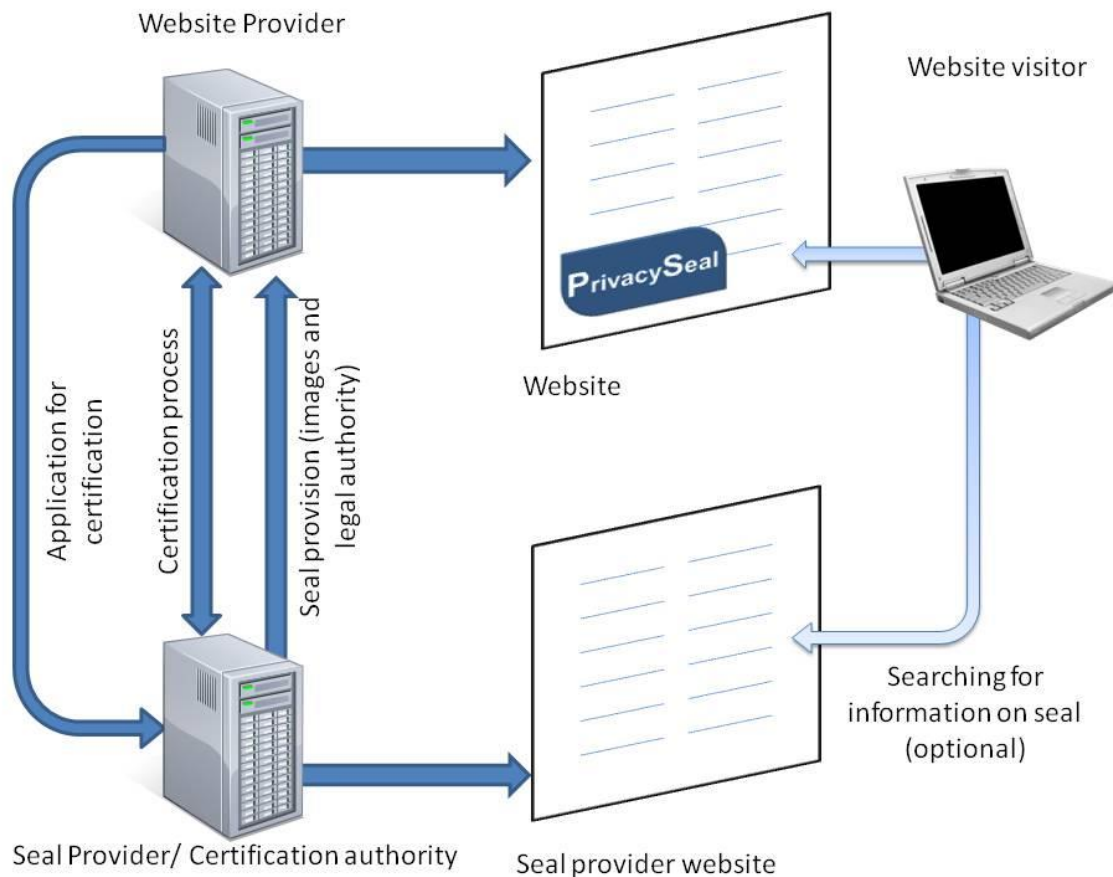


Figure 4: Classic or minimal seal model

Typically, a website wishing to become part of a seal scheme makes a request for certification to the seal provider. This initiates a certification process which, if successful, results in the seal provider granting the website the use of the seal. The seal is then displayed to visitors to the website, as part of the website.

If the website visitor desires more information on what the seal certifies or claims, then this is available from the website of the certification company. This model is not restricted to privacy seals, and can be used for any type of website certification. In many cases, the visitor will not seek any more information on the seal.

The key issue with this model is the ease with which the seal can be impersonated (it is an inactive, unlinked image file, which can easily be copied). Similarly, revocation (following the end of the contract or a violation of the programme requirements) in this model cannot be automatic, and the website must co-operate in the removal of the seal. The relationship between the seal provider and the certified entity is weak, and hard for the website visitor to interrogate.

Linked seal

The linked seal model builds upon the classic seal model by turning the seal itself into a hyperlink to information on the seal scheme, typically hosted on the website of the certification authority. A visitor that desires more information on the seal scheme can find this more easily than in the classic model. This increases the linkage between the certification authority and the certified entity.

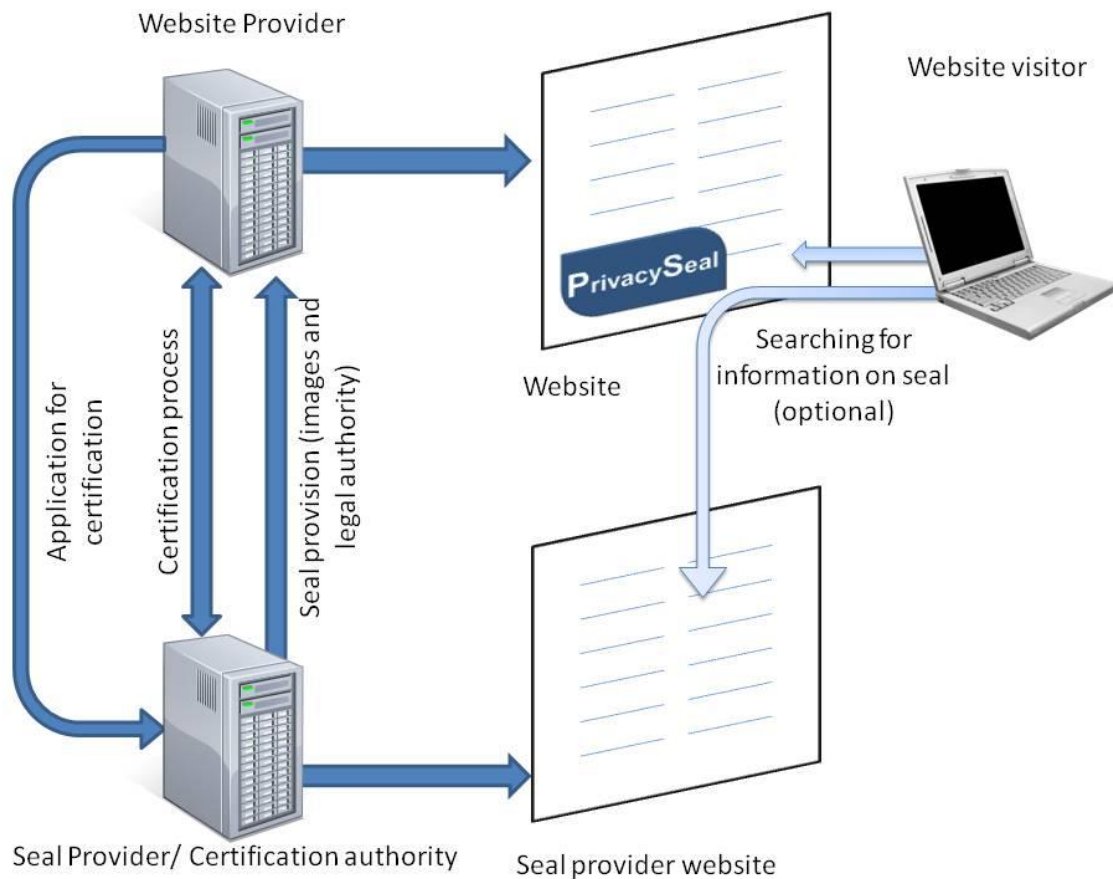


Figure 5: The linked seal model

A continued criticism of this model is that the information provided is generic and not linked to the specific certified entity; this is clearly an issue when the certified entity has some flexibility as to the certified perimeter, as is frequently the case. The seal scheme has to police incoming links, and be aware that its information might be linked as part of a fraudulently displayed seal. The seal displayed on the website is still under the control of the certified entity, and the link could easily be broken, non-functional or misdirected. Another criticism is that the seal provider website may be largely promotional for the seal scheme itself, rather than providing information on the scheme member.

Hosted seal

The hosted seal model attempts to overcome the limitations of the classic and linked seal models. It is therefore the most common seal model amongst those analysed. It also forms the basis for a number of subsequent variants. In this model, the seal image is hosted to the website visitor from servers controlled by the certification authority. Typically, the seal also contains a link back to the certification authority.

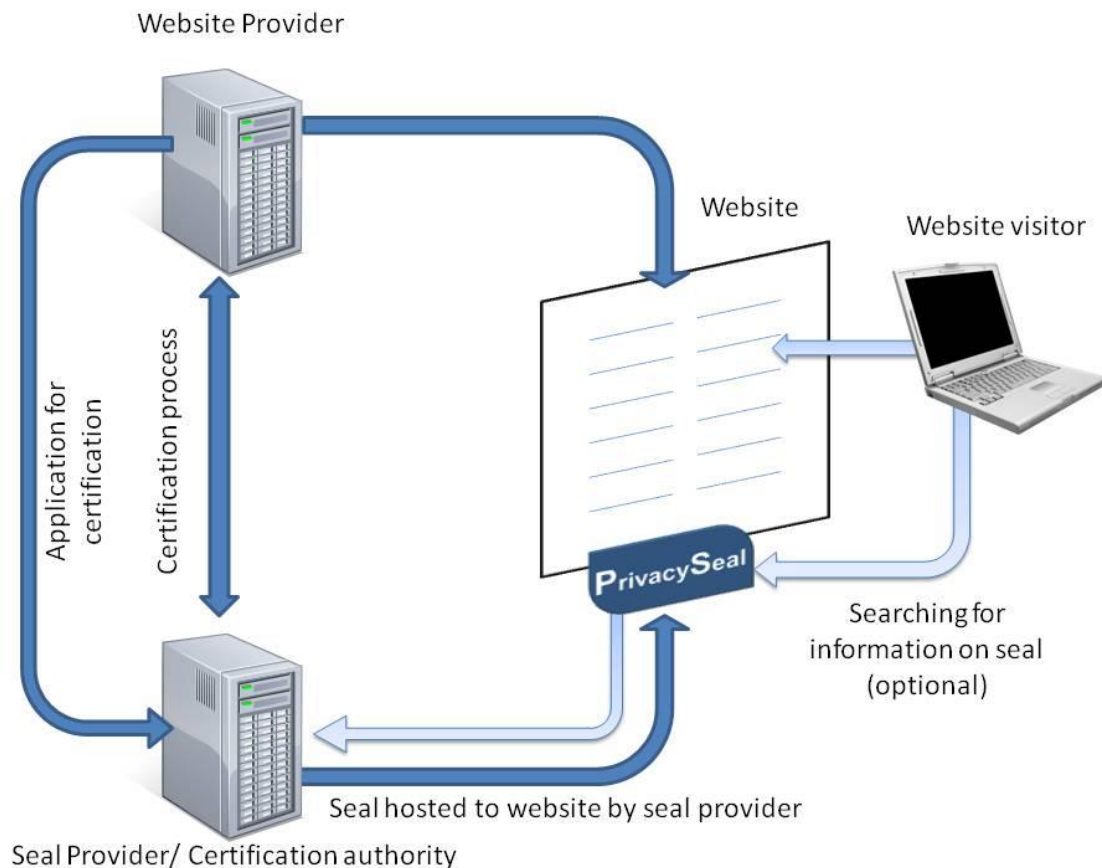


Figure 6: A hosted seal model

Because the seal provider retains control over the hosted seal, automatic revocation is now possible. If the seal provider believes that the website has violated the programme requirements (or otherwise invalidated its agreement), it can decline to host the seal, and no seal will appear to the visitor to the website.

Hosted seals are often unique for each certified entity in the scheme. They can therefore link back to a specific page on the certification authority's website, with details about the status of that particular certified entity, how long it has been certified, or other useful information. Additionally, a hosted seal might also allow the seal provider to collect personal data from the visitor.

External standards seal

The external standards seal is a variation upon any other form of seal model (the diagram below shows an external seal variant of a hosted seal). What differentiates this model from others is the content and origin of its standards rather than its mode of presentation. In this model, rather than the certification authority creating its own standard or code of conduct, and certifying applicants against this, the standard is provided by some external authority (perhaps a law or industry standard). The certification authority has no control over the standard, but has been entrusted to certify third parties against this standard (there is possibly some application process here to determine if the seal provider is adequately performing its task).

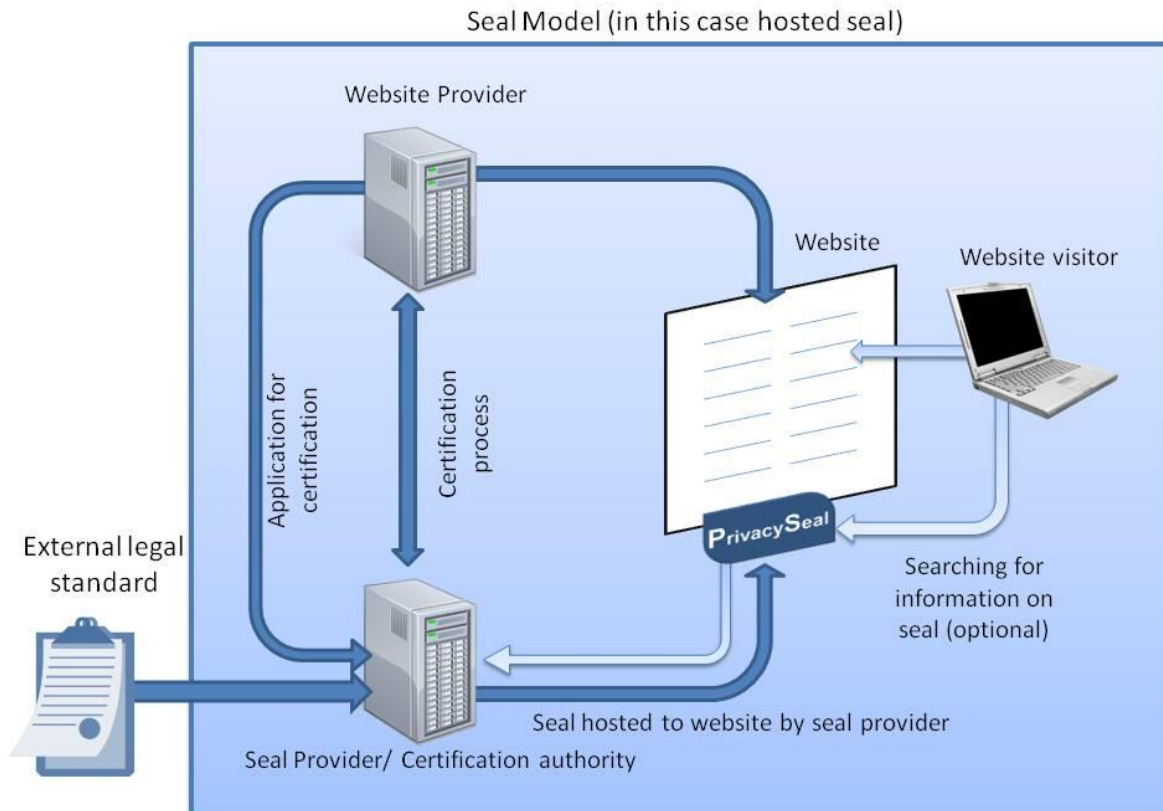


Figure 7: External standards seal model

The legitimacy or value of seal schemes using this model is strongly tied to the legitimacy of the external legal or technical standard. Meeting a legal standard may be mandatory for a website, but the certification is more likely to be voluntary.

Delegated certification

This model of seal was only identified with regard to WebTrust, but the model has some potentially general applicability. In this model, the seal scheme empowers specific types of independent third parties (chartered accountants in Canada and certified public accountants in the US in the WebTrust case, and independent experts with appropriate qualifications and experience who have undergone reliability checks for EuroPriSe) to conduct the certification process on its behalf. The results of the certification process are relayed back to the seal provider and, if appropriate, the certified entity is provided with the right to use the seal. The seal authority maintains a register of certified entities. This could also be understood as a certify-the-certifier approach.

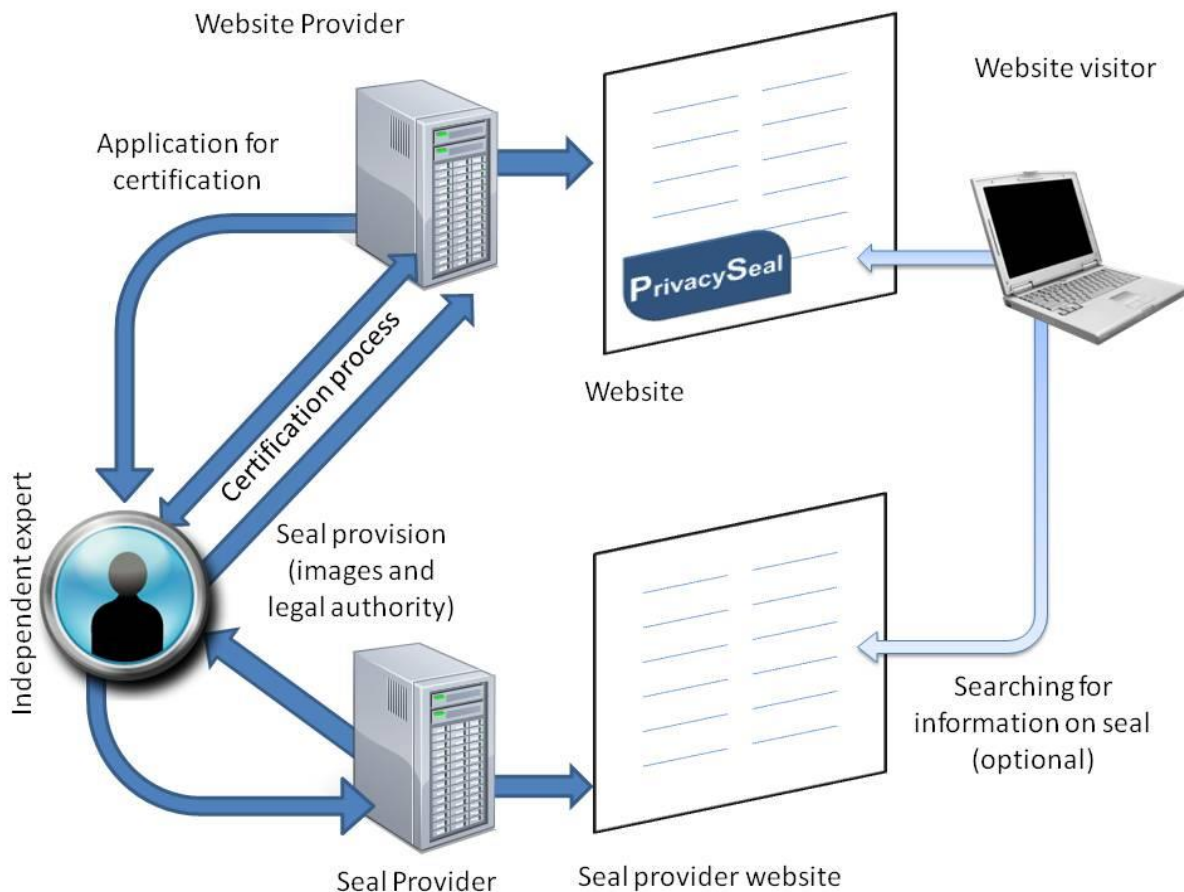


Figure 8: Delegated certification model

This model could also be integrated with a hosted seal, but was not in the case of WebTrust. The difference between this model and the external standards model above is that in this model there can be a large number of assessors, while the seal provider still plays the role of standard-setting agency. A point of variation is how institutionally “close” the independent expert is to the seal provider or to the certified entity.

A potential criticism of this model is that the one of the actors in the certification process (the chartered accountant or independent expert) is not visible to the public or the website visitor. Similarly, the seal provider must have some method for oversight of the independent third parties; therefore this model effectively requires two certification processes.

Federated seals

In the federated seals model (depicted here as a federation of hosted seals), multiple certification authorities agree amongst themselves on a shared standard (often a shared minimum standard).

This model allows smaller national level (or potentially industry sector) schemes to benefit from the increased recognition that comes with a larger scheme, without abandoning particular local concerns, provided that the multiple certification authorities can agree a common standard.

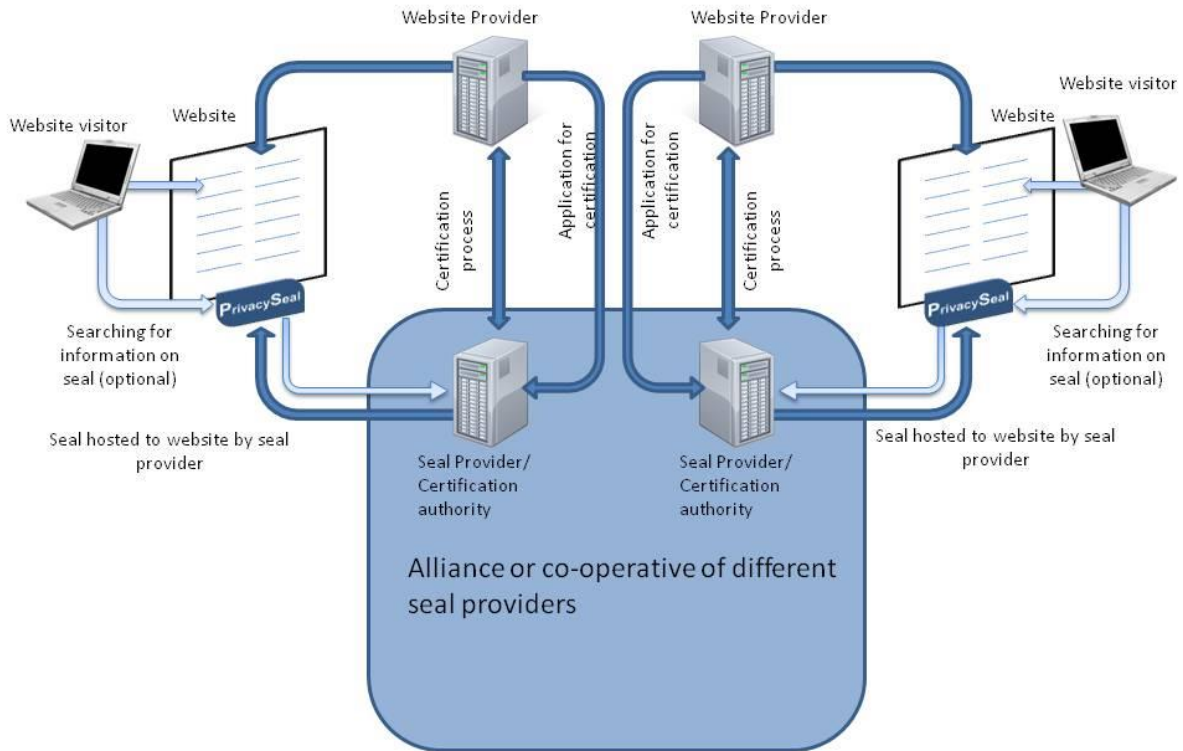


Figure 9: Federated seal model

Security scan seals

Security scan seals vary the certification process of the hosted seals model. Rather than an initial certification process with an annual or bi-annual re-certification, in this model, the certified entity is effectively re-certified every day, through a security vulnerability scan conducted by the seal scheme. If the vulnerability scan produces a negative result, the seal is displayed to any visitors to the website. If security problems are identified, then the website provider is informed and given advice on corrective actions that can be taken. If no corrective actions are taken, then the seal can be removed in a relatively short time frame.

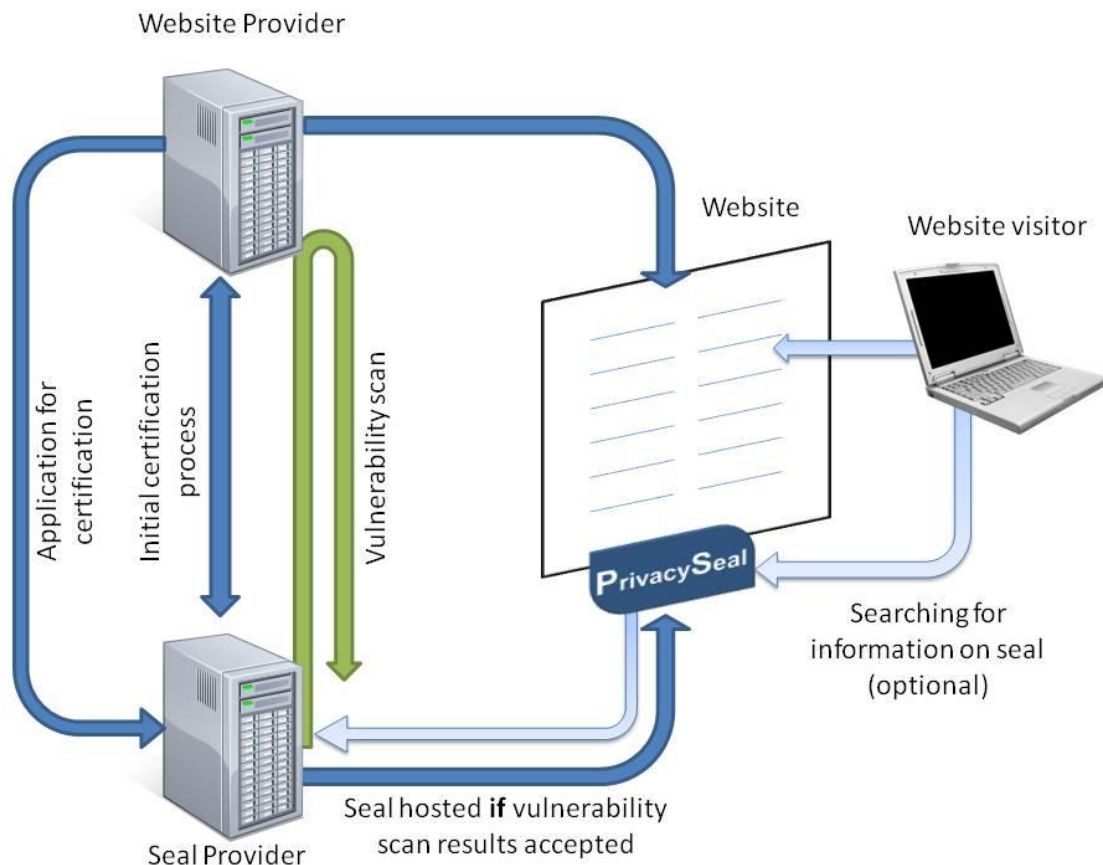


Figure 10: Security scan model

Given the frequency of scans, the vulnerability scan is automated. It uses proprietary technology and knowledge of security vulnerabilities to look for ways in which the certified website is vulnerable to attack. This scan therefore has a technological and security focus. It does not address processes of information-handling or compliance with the law. This limits the extent of what can currently be certified by such a seal model.

These models are often supplied as part of a security service. The seal therefore signifies to the visitor that the service is being provided.

Insurance seals

Insurance seals add to an e-commerce website the opportunity for the visitor to purchase additional insurance protection. Rather than certifying that certain security or data protection measures have been taken, the seal guarantees that if identified problems do arise, then the customer will be protected. The insurance product is typically added to a transaction for a low optional cost paid for by the purchaser, or to all products sold on the website with the cost carried by the website provider. If the visitor encounters a problem covered by the insurance policy, she can make a claim against it.

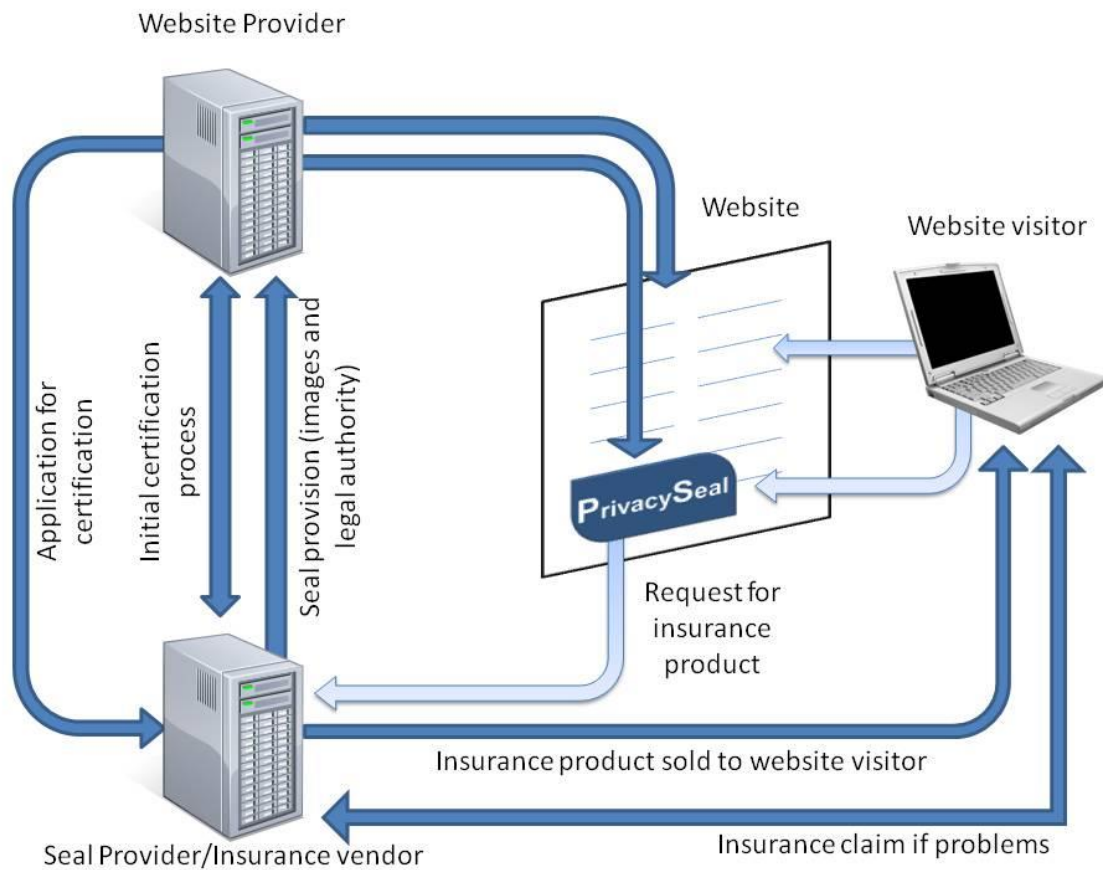


Figure 11: Insurance seal model

This model works on an economic liability shift. In most seal schemes, the certification authority asks the user to trust that it has done adequate certification work to be able to hold certified entities to its standards. Whilst it may be possible to hold other seal schemes legally accountable if a certified entity does not adhere to the certification requirements, the liability shift is not explicit, and is not the cornerstone of this model. In the insurance seal model, the incentive is on the insurer to conduct adequate due diligence to minimise the number of insurance claims for which it has to pay out. Rather than trusting the certification process, the website visitor is asked instead to trust that they insurer will pay out on valid claims. The driver of data protection efforts, if any, is the desire of the insuring party to minimise their pay-outs by only insuring (and granting a seal to) websites that meet their internal (and often undisclosed) standards. It may be possible to combine an insurance model with other types of seal mechanisms, although currently existing insurance seals tend to offer their service only to active customers, rather than non-paying visitors to websites.

These schemes tend to focus upon the commercial shopping experience. Problems that can be insured against include purchased products not arriving on time, or at all, or not being as described. BuySAFE, which uses this model, offers identity theft protection insurance for 30 days following the transaction.

This model works for commercial websites, where the intention is to make a sale. If there is no transaction occurring, then it becomes difficult to insure the website user. It is also problematic in relation to data protection harms that cannot easily be quantified and damages that cannot be financially compensated. The model is also strongly dependent upon how well the available cover fits with the likely harms. Compromised credit card information is often

held for some time before being exploited, and it often takes a victim time to determine that they have been victimised, meaning that 30 days' protection may not be sufficient.

Registry

In the following two models, the certification authority maintains a register of information on certified entities. This register is accessible to the intended audience of the scheme (in practice, this is online and public, but these registers could also be private or membership-based). These schemes are differentiated from classic or linked seals in that they generally do not provide a seal per se. However, they function in a similar manner. The disadvantage of both models is that the website visitor or service user has to be aware of the existence of the registry.

Self-assessment register

In a self-assessment register (as in the model used by CSA), the service provider completes a self-assessment form and deposits this with the registry, which then makes it publicly available. The registry likely depreciates or removes information that has aged beyond a set time limit.

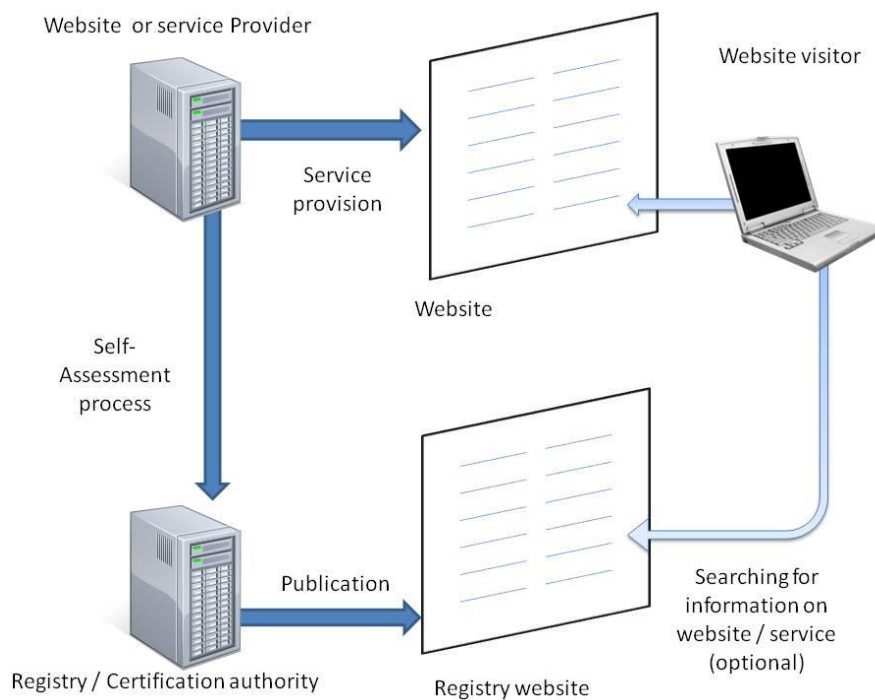


Figure 12: Self-assessment register model

Investigative registry

An investigative registry is similar, but in this case compiles its own information on websites or service providers, and then makes this information publicly available. None of the analysed schemes made use of this model, but it is included here as a possibility. This registry could be considered as a white-listing or review system. The method by which such a registry could conduct its assessment procedures is fairly open, and could even involve crowd-sourced information.

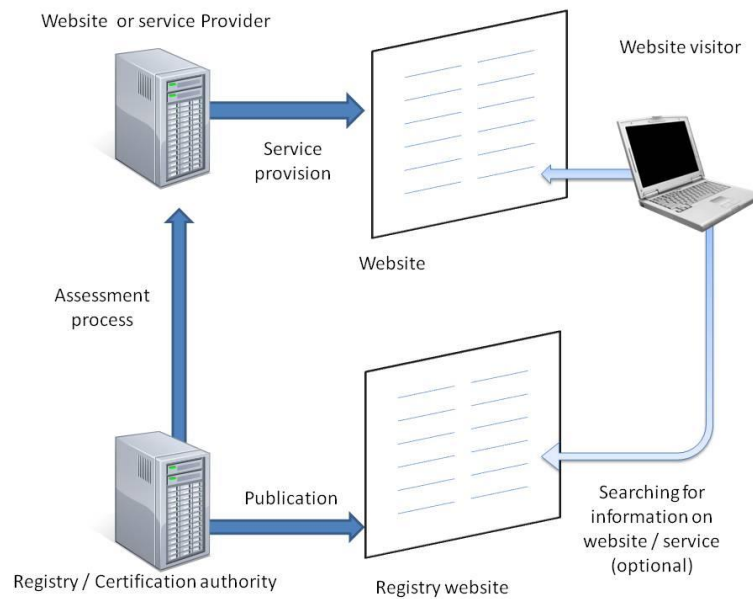


Figure 13: Investigative registry

3-D Secure model

3-D Secure is the name for the technology protocol used by Verified by Visa, but also by MasterCard SecureCode, JCB International J/Secure and American Express SafeKey. Rather than a privacy seal, 3-D Secure should be understood as a transaction security method. The name derives from the three domains involved (the merchant or bank to which money is being paid, the card issuer that issued the card, and the interoperability domain provided by the card scheme).

Verified by Visa allows participating online retailers to offer an additional password-protected stage to online card transactions. A user makes an application for a credit or debit card from a participating card issuer. When they attempt to use this payment card online with a participating retailer, the retailer (or their online payments provider) redirects the customer to their card-issuing bank, to provide additional information (a number of letters or digits from a longer password) before authorising the transactions. This provides the retailer with an authorisation code they can later provide to the bank. The password is not revealed to the website provider. This is claimed to provide greater security for the card user.

The way that a user signs up for the process (and resets passwords) is left to the discretion of the card-issuing bank, but often occurs during the online transaction itself. Some banks mandate that card users sign up for Verified by Visa if they wish to conduct online transactions.

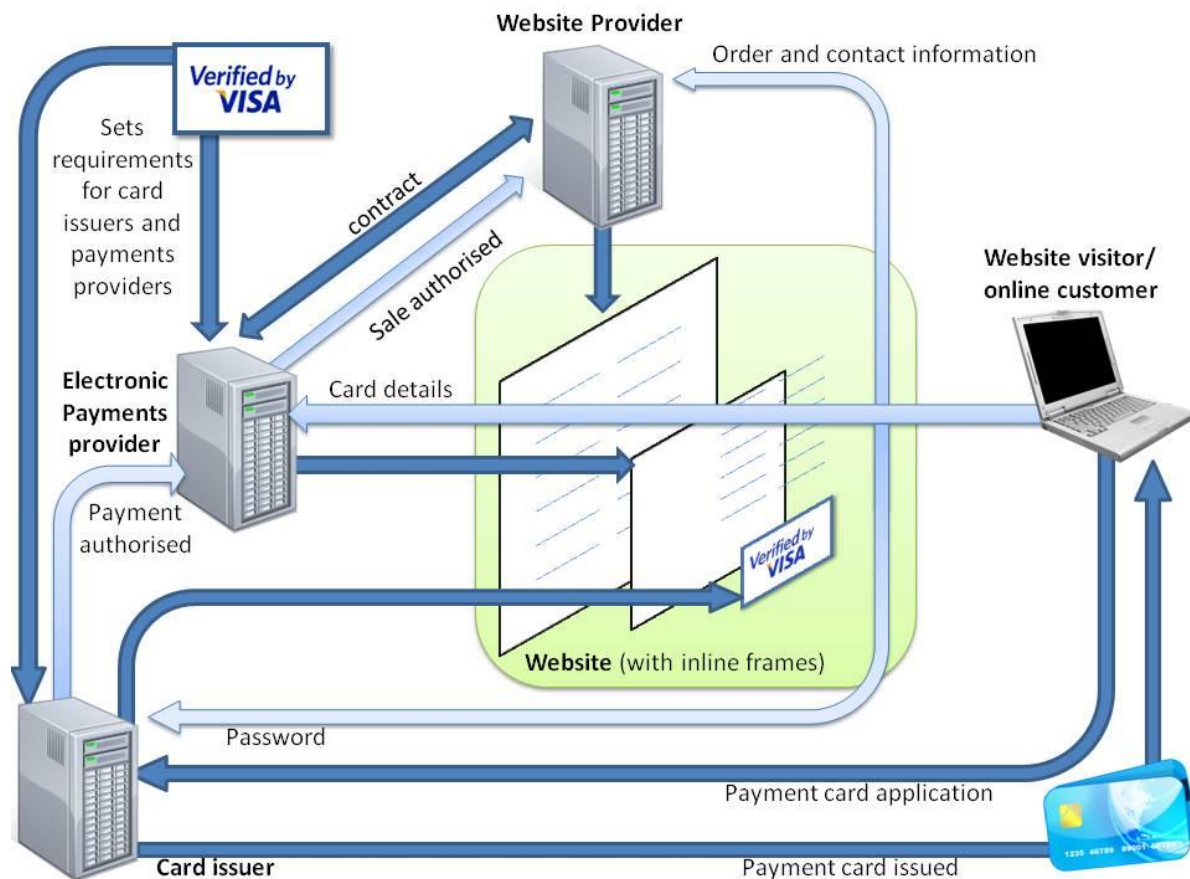


Figure 14: 3-D Secure model

There have been several criticisms of this now-widespread model. The instruction to provide personal information and payment card details to an unexpected and redirected web page may train users to take a generally unsafe action. Under this scheme, the user may experience very different procedures of verification depending on the entity using the model. This is disturbing for customers, especially when they are asked for bank account details. To the extent to which the website attempts to hide the complexity of the model, it can be seen as reducing the amount of information available to the users. The incentive model has been criticised as primarily concerned with shifting liability for rejected or fraudulent transactions away from the bank and merchant and towards the card user. With some banks imposing use of the process onto their customers, the scheme cannot be considered fully voluntary. Finally, the password reset method is quite vulnerable.

Whilst not focused upon privacy, the 3-D Secure model does demonstrate a way in which a number of actors in a network can provide partial data which can be checked against other data held by other actors, without revealing all the data to all participants. Systems such as this could potentially be set up to guarantee that certain privacy-protecting actions have been taken.

Combination of seal models

It is possible for a website to be a member of multiple seals schemes and many do display several. The diagram below demonstrates the complicated set of relationships surrounding a website that has a 3-D Secure payments process, and a security vulnerability scan. This model

could be further complicated with the addition of a seal focused upon data protection and privacy.

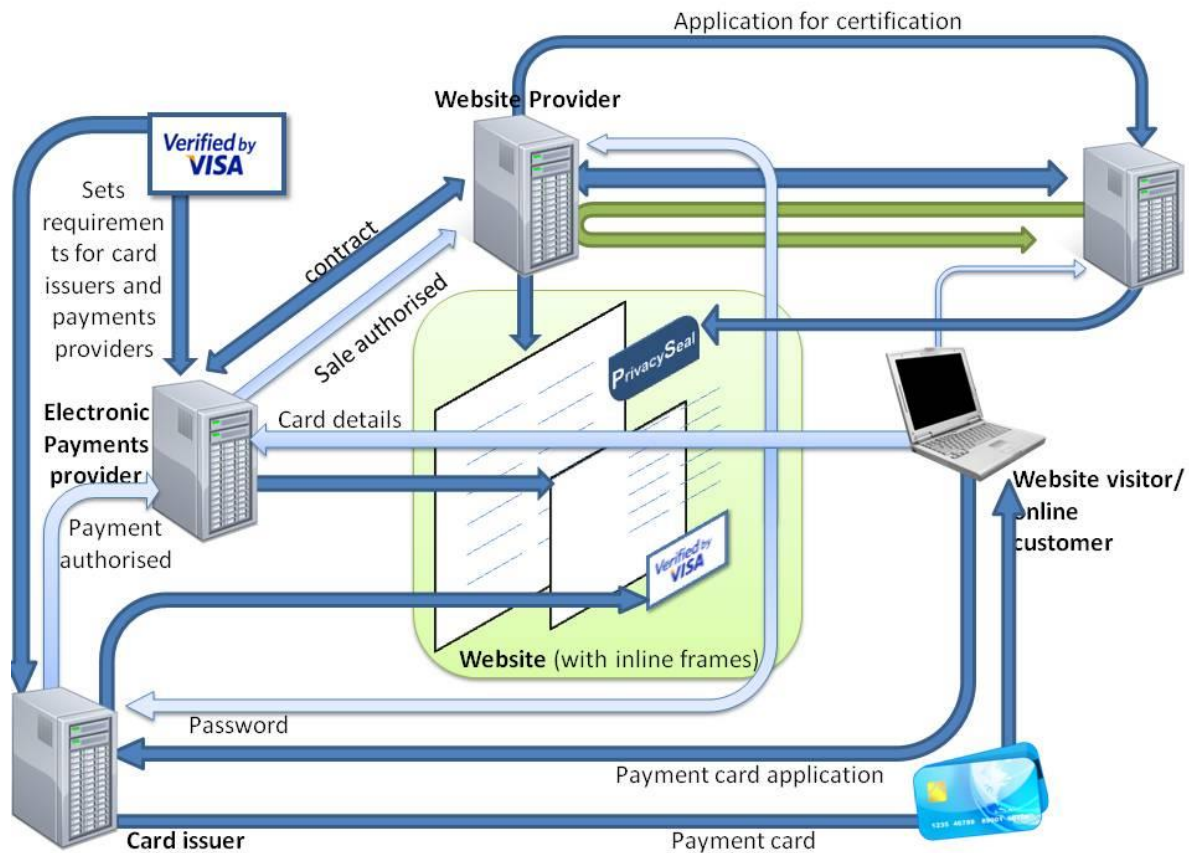


Figure 15: Combination of seal models

The typical privacy seal

It is important to understand the elements that privacy seals have in common as well as the elements that distinguish them. Understanding the most common elements of privacy seals allows us to identify areas that may be stable or resistant to change, and what might be considered the core characteristics of privacy seals. It also allows us to identify areas of high variability, and as such that might be more easily changeable. This section maps the characteristics of the analysed seals against each other, producing a set of distinct “fingerprints” for each seal. Bringing those fingerprints together for comparison allows us to identify commonalities between seals and to identify the typical privacy seal.

The following table plots the characteristics of each seal against the categories developed during the analysis against the general criteria in Section 5.1.

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	unknown	small	Organisations	yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	contact email only	medium	websites	no
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-	Legally Aligned	compliance with law	member first	large	systems	
External Standards Seal	Security		Canada	Professional representative body (industry association)	Detailed	detailed	scheme first	very large		
Delegated Certification Seals			Europe		Granular	highly granular				
Federated Seals			France			Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

Table 15: Categories for key variables

Filling in this table for a given scheme provides a “fingerprint” for that individual scheme. For example, the following table depicts the Cloud Security Alliance scheme:

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

Table 16: CSA scheme characteristics

The next table plots characteristics for the Confianza Online scheme (cells marked in blue):

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for-Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

Table 17: Confianza Online characteristics

These images allow visual comparison between two or more schemes. “Fingerprints” for all schemes are included in Annex II. The two most similar seals are TRUSTe and ESRB. The distinctions are that TRUSTe is a private company, whilst ESRB is a not-for-profit, and that TRUSTe provides detailed guarantees to the data subject, whilst ESRB does not.

Layering the individual “fingerprints” produces a density map of the characteristics of the analysed schemes as depicted below. The darker areas represent more common features among the 25 reviewed seals.

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	scale (very large/ large/ medium/ small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (international)	Data protection authority	Abstract	Abstract	Contact email only	Medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (domestic)	Not-for-Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards Seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information Security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							



Table 18: Density map of the shared characteristics of the analysed schemes

Based upon the density map, the typical privacy seal can be described as follows. The typical privacy seal is a hosted seal, where the seal logo is served to the member website directly from the seal provider, and can be revoked by the provider. It is a privacy seal, in that it makes some claims about data protection and privacy issues. It is likely based upon a standards verification model, where the practices of the scheme member are held against a fixed standard. It is highly likely to be operated by a private company in the United States (or a national scheme limited to a specific European Member State). The actual data protection and privacy elements of the scheme are likely to be under-detailed, with limited information available, and the scheme is unlikely to make specific guarantees to the data subject themselves. The complaints process may not be very transparent, with perhaps only an e-mail address to contact. The scheme is most likely to have a small to medium number of certified entities (no more than the low thousands). The scheme is more likely to certify an organisation's practices as a whole, rather than specific websites, and it is unlikely to use external experts.

Other seal schemes can be compared against this typical model. For example:

TRUSTe

The TRUSTe seal is close to the typical seal model. It is a hosted, privacy seal, based upon a standards verification certification process, administered by a private company based in the US, but applicable internationally. It does, however, have a number of areas of divergence. As a medium-scale seal, it is larger than several other schemes with similar models. Its complaints process directs people towards the scheme member first, with TRUSTe as a dispute resolution process. It has more detailed data protection and privacy elements, and a more detailed set of guarantees for the data subject than the typical seal.

Verified by Visa

Verified by Visa is by far the largest of the analysed seal schemes with more than 300,000 certified sites in Europe alone. It is twice the size of the second largest scheme analysed (BBB Accredited Business Seal). It is also highly divergent from the typical privacy seal model. It is based upon the 3-D Secure model, is primarily a security seal, with little coverage of the data protection practices of certified entities beyond information security (primarily handling of payment card and financial transaction information). Many of its requirements focus upon increasing the assurance that payments are non-fraudulent. It is a service scheme, often provided to websites through their payments provider and often requiring advised changes in software, hardware or protocols. It is a global service, although with some regional variations.

The few areas of convergence with the typical seal are that it is administered by a private company, offers no specific guarantees to the data subject (although it does offer guarantees to the scheme member in relation to card-not-present fraud charges), and does not use accredited experts. Although payment providers function in this role to a certain extent, it is VISA's own testing system that makes the final application decision. The complaints and redress procedure is not immediately transparent. Verified by Visa also has a very different relationship with the website visitor than other seals. The use of Verified by Visa can be mandated by the visitor's card-issuer and bank. Functionally, the process also re-directs information submitted by the visitor, and requires additional information from them in the case of a purchase. When compared to other seal models, the visitor is effectively required to interact with the Verified by Visa seal. Other seals can be ignored.

7.2 SCHEME OBJECTIVES

Section 6.3.9 demonstrated that the objectives of schemes tended to cluster around six categories: building confidence or trust, signalling compliance or accordance with a standard, signalling the presence of data protection measures, providing guarantees, increasing market transparency and resolving disputes. Several of these objectives relate to the message that the seal is attempting to convey.

Seals are about conveying a potentially complex set of information in a very rapid and simplified way. Most users of a website will not interrogate a seal and what its objectives are in much detail, if at all. Many seal schemes make use of linked seals to put information about the seal apart from the seal, but accessible through it. However, several do not disclose sufficient information. This is related to the way that seals function.

Building confidence and trust is a stated objective for several schemes, but is most strongly associated with e-commerce and general trust marks, rather than specialised privacy seals, which tend to focus upon specific data protection measures. Commercial confidence and trust is associated with domestic rather than regional or international scope. Some of the general confidence-building schemes are amongst the larger seal schemes. Schemes focused upon signalling compliance with a standard are more likely to provide more granular and detailed information about that standard and those schemes where the objective is increasing trust and confidence. Abstracted or general claims allow a seal to evoke a broader sense of trust and confidence than its technical organisation, certification process and applicable standards might warrant.

All of the subsequent objectives can potentially contribute to increasing trust and confidence in a more specific, more transparent way.

7.3 EU SCHEMES AND NON-EU BASED SCHEMES

The following two density maps collate the scheme characteristics for the United States and Europe respectively. Comparing the US and European seal schemes analysed in this study yields the following points of convergence and divergence.

Hosted seals are the most common in both regions. Europe has a federated scheme (Euro-Label) whilst the US has insurance, registry and security scan schemes. The latter two types are available to EU entities and users. The US potentially supports a broader range of seals than Europe. The sample also includes more dedicated privacy seals from the US. US seals are more likely to be administered by a private company (although this is still the most likely option in Europe). Unlike the US, Europe has seals administered by data protection agencies. Both regions have seals run by non-profit, non-governmental bodies. Standards verification seals are the most common certification process in both the US and Europe. Both consultancy schemes are based in the US. US seals are more likely than European seals to have poorly detailed data protection and privacy elements, or focus solely upon information security and to make no specific guarantees about the rights of data subjects. European seals are more likely to be aligned with a legal standard for data protection and privacy and to make guarantees of compliance with such laws. For those European seals aligned with a specific legal framework, the relevant framework is EU Data Protection law. As such, European seals

are less likely to have abstract guarantees. European schemes are slightly more likely to have complaints processes in which the complainant is requested to contact the scheme first, and for the scheme to take up the complaint with the scheme member, than the US, where it is more likely that schemes will request complainants to contact the scheme member first. Europe has no large or very large-scale seal schemes. Most of the schemes in both regions are small in scale. There is no real difference between the two regions in relation to expert certification. It was difficult to find information on the extent to which the European schemes certified websites or organisations (two schemes explicitly certified systems, which was not the case for any US schemes). US schemes tend to certify organisations.

The table below illustrates the characteristics of the US-based seals:

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	scale (very large/ large/ medium/ small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	Medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards Seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information Security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

Table 19: Characteristics of the US-based seals

The table below illustrates the characteristics of Europe-based seals:

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	scale (very large/ large/ medium/ small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	Medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for-Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards Seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information Security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

Table 20: Characteristics of the Europe-based schemes

7.4 COMPLIANCE AND REGULATORY STANDARDS

Most of the schemes analysed are based upon a standards verification model of certification, where applicants are assessed against a pre-existing standard. A small number of outliers offer consultancy services where they provide advice and assistance in setting up data protection or information security practices, potentially including drafting a privacy policy. Amongst the standards verification seals, there is a distinction between compliance with an internal standard developed by the seal, and with an external standard created by an external authority.

	USA	Europe
Internal standards	CSA, Gigya, Smart Grid Privacy seal, McAfee SECURE, TRUSTe, Verified by Visa, WebTrust	Comodo, Confianza, Euro-Label, TÜViT Trusted Site Privacy Certification
Internal and external standards	BBB Accredited Business Seal, ESRB	MRS Fair Data, Trusted Shops
External standards	PRIVO	CNIL label, ePrivacy seal, EuroPriSe, Seriedad Online

Table 21: Standards and schemes

There are a wide range of compliance and regulatory standards to which seal schemes refer. Internal standards include examples such as the BBB Code of Business Practice, the Confianza Ethical Code and the MRS Code of Conduct. External standards are typically the appropriate data protection and privacy law for the jurisdiction in which the seal is based and operates. ESRB represent a divergence from this pattern. It is based in the US, and is generally concerned with applicability of US law; however, one of its seal offerings demonstrates compliance with European Data Protection law for US-based entities wishing to do business in the EU. The internal standards of some schemes incorporate a range of legal standards (for example, combining privacy and data protection with consumer rights). It is, however, the internal standard against which applicants are assessed. Directive 95/46/EC is a regulatory standard for several schemes operating across the EU (ePrivacyseal, ESRB, and EuroPriSe). National-level seals tend to reference their national level data protection law (MRS Fair Data, CNIL label, Seriedad Online, ePrivacy seal).

Schemes that simply demonstrate compliance with a single law are comparatively rare, and in both cases (PRIVO and an ESRB seal) signal compliance with the US Children’s Online Privacy Protection Act (COPPA). The relative scarcity of this type of seal may be explained by the relatively low “value-added” by a seal scheme on top of mandatory legal compliance. The appearance of COPPA certifying seals is a result of the US Federal Trade Commission setting up a process for delegated certification through COPPA Safe Harbor providers, and because COPPA relates to websites that are targeted at children under 13, something which might not be apparent from initial inspection of a website. Therefore, a COPPA seal signifies that not only is the site COPPA compliant, but that it also suitable for children under 13. Outside of the field of privacy, Seriedad Online, McAfee Secure, BBB, and buySAFE refer to compliance with laws in other fields, particular relating to commerce and e-commerce (see section 6.3.19 for details).

Larger seal schemes engage with a problem of cross-jurisdictional applicability. Generally, the more a scheme is available across legal jurisdictions, and is targeted at an international audience (which correlates loosely with a larger number of certified entities), the less likely it

is to signal compliance with a specific law or regulatory framework, and the more likely it is to assess membership against an internally derived set of criteria. A second solution to this issue is the federated seals model used by Euro-Label, where individual national seals comply with Member State requirements, but the scheme as a whole agrees a set of common minimum standards for membership.

7.5 RIGHTS OF DATA SUBJECTS

The typical seal scheme presents an under-specified set of rights for the data subject, as well as non-specified guarantees. There is a tendency to discursively construct the protections offered to the data subject by the seal scheme in a manner that parallels but is not conducted in the language of data subject rights. Therefore, several schemes state their commitment to the protection of personal information, and ensuring that it is used in a transparent way, with opportunities for consent or opt-out. The absence of use of the term “data subjects” in relation to specific rights may be the result of the dominance of US-based seals.

One reason for this expression of rights may arise from the incentives of running a seal scheme. If a seal simply recognises rights that are already understood to exist, regardless of a website or organisation’s commitment to them, then it may be understood as having less independent authority, and therefore be of less interest to potential members. Abstract or poorly detailed data protection and privacy elements allow for a degree of flexibility in an area where assessing privacy and data protection practices can be complex.

Specific guarantees to the data subject are uncommon in seal schemes. Some schemes explicitly state that they do not provide a legal guarantee or warranty. This claim may have variable validity in different legal jurisdictions and raises related issues of enforcement and legal liability. There may be a number of reasons for this ranging from a lack of a contractual or legal relationship between the seal scheme provider and the data subject, liability issues or the functional inability of a scheme to offer such guarantees. buySAFE is an outlier in that the entire scheme is based around an insurance model, in which additional guarantees are made to the customer, but through their role as a paying customer rather than as their inherent status as a data subject.

EuroPriSe appears to offer the greatest level of guarantees to the data subject.

7.6 COMPLAINTS REDRESS

The key convergences and divergences in the areas of complaints and redress have been identified in section 6.3.22. The following tables show the different types of complaint mechanism against the nature of the scheme, the data protection and privacy elements, and against the nature of the certifying entity. This section assumes that the primary complainant is a website user/person relying upon a seal.¹¹⁵

¹¹⁵ Many schemes, especially those with contractual relations between the certification authority and the certified entity, will likely have an internal mechanism for communication between the parties, for example a customer relations department or sales advisor.

Nature of scheme/ Complaints mechanism	General	Privacy	E-Commerce	Security
None/Unknown	E-mark, Euro-Label	Gigya, ePrivacyseal, Transaction Guard, Trustify-me, WebTrust		
Contact e-mail		EuroPriSe, CNIL Label, TÜViT Trusted Site Privacy Certification	buySAFE	McAfee, Verified by Visa
Approach member first		ESRB, MRS, Smart Grid Privacy seal, TRUSTe		
Approach scheme first	BBB Accredited Business Seal, CSA, Confianza, Seriedad	PrivacyMark System, Privo		Comodo
Member must have complaints mechanism		TÜViT Trusted Site Privacy Certification	Trusted Shops	

Table 22: Complaints mechanisms and nature of the schemes

The following table illustrates the complaints mechanisms in relation to the privacy and data protection elements of the analysed schemes:

Data protection and privacy elements/ Complaints mechanism	None	Abstract	Legally aligned	Detailed	Information Security
None/Unknown		Transaction Guard, e-mark, Gigya, Trustify-me	ePrivacyseal, Euro-label	WebTrust	
Contact e-mail	buySAFE	CSA	EuroPriSe, CNIL Label	TÜViT Trusted Site Privacy Certification	McAfee, Verified by Visa
Approach member first		MRS, Smart Grid Privacy seal		TRUSTe, ESRB	
Approach scheme first	BBB Accredited Business Seal, Seriedad	PrivacyMark, Comodo, Confianza	PRIVO		
Member must have complaints			Trusted Shops	TÜViT Trusted Site	

mechanism				Privacy Certification	
------------------	--	--	--	-----------------------	--

Table 23: Complaints mechanisms and privacy and data protection elements

The following table illustrates the complaints mechanisms in relation to the nature of the certifying authority:

Nature of certifying authority/ Complaints mechanism	Private Company	Data Protection Authority	Not-for-Profit	Professional body
None/Unknown	ePrivacyseal, Gigya, Trustify-me, Transaction Guard, WebTrust		e-mark, ESRB, Euro-Label	
Contact email	buySAFE, McAfee, TÜViT, Verified by Visa	CNIL Label, EuroPriSe	CSA	
Approach member first	Smart Grid Privacy seal, TRUSTe			MRS
Approach scheme first	Comodo, PRIVO, Seriedad Online		PrivacyMark, BBB Accredited Business Seal, Confianza	
Member must have complaints mechanism	Trusted Shops, TÜViT Trusted Site Privacy Certification			

Table 24: Complaints mechanisms and nature of certifying authority

Too many of the analysed schemes do not provide a detailed explanation of their complaints procedure or limit the information available to an e-mail or web-form, with no information on what a complainant (e.g., website user/person relying on seal) can expect. This includes schemes administered by data protection authorities. The relatively large number of unknown processes makes the following analysis of complaints and redress processes tentative.

Security-focused seal schemes, where data protection elements are limited to information security, tend to provide only a general contact e-mail for complaints. Verified by Visa and McAfee secure are primarily providing an information security service to the website owner, and there may well be internal complaints mechanisms open to these subscribers that are not facing the general public.

Where information is available, the general trust seals all encourage the complainant to approach the scheme first in making a complaint.

There is some convergence between schemes with poorly detailed data protection and privacy elements and schemes with none or unknown complaints procedures. This likely signifies a generally limited amount of information available on those schemes.

The complaints mechanisms for schemes administered by private companies are broadly evenly distributed across the categories, whilst not-for-profit schemes converge around contacting the scheme first in the event of a complaint.

However, the fact that a complaints or dispute resolution mechanism exists does not necessarily mean that it is acceptable, usable or sufficient from the consumer point of view. In many instances, dispute mechanisms appear fully internal and do not foresee the participation of independent entities nor consumer representatives.

With regard to schemes that state that they are aligned with some form of legal standard, but for which we were unable to find a complaints procedure, this might suggest that they fail to adequately meet some of the legal requirements, particularly of EU data protection. If an entity is processing personal data, then it must have a public data protection contact; however, this requirement may not fall upon privacy seal schemes if they are not processing personal data, but rather commenting on the personal data processing of another entity.

7.7 SHARED PROBLEMS

Whilst it is possible to characterise a typical model, and then compare existing seals (and potential future seals) against it, the density map does also demonstrate some of the variation in the field. Whilst there are common models of seals, and shared ways of operating a scheme, the variation in the details is important. It raises the question of what exactly each scheme is certifying, the difficulty of understanding this, and the accessibility of this information to users. Without close examination of a seal scheme, it can be difficult for a user to understand what exactly a given seal scheme is certifying. Certain schemes certify a particular website, others the company or organisation behind the website, and others (McAfee) can certify a particular web page or IP address.

The analysed schemes can be characterised as broadly clustering around few common models, however, with a large diversity in the implementation of those models. This raises issues of understanding and evaluation of individual privacy seals. In the absence of detailed information on a given seal, anyone attempting to understand what a seal signifies is likely to rely upon the scheme resembling other seals, which may be erroneous.

7.8 GDPR REQUIREMENTS

With regard to the GDPR criteria, the fact-finding analysis has illustrated a number of points of convergence and divergence among them. Here again, however, a main distinction needs to be made between EU-based and non-EU schemes; while the former approximate as best as possible the GDPR criteria, these criteria in their specific form seem less relevant to the non-EU schemes.

In any event, in regard to the points of convergence among EU-based schemes, the first point that has been highlighted in the preceding analysis (section 6.4) is their lack of preparation as far as the draft GDPR novelties are concerned. No analysed scheme in operation in the EU today has moved towards the prospective rights of data portability and the right to be forgotten. The same more or less is true of other GDPR novelties, such as data protection impact assessments, the principle of accountability or, with some exceptions, the special

protection afforded to minors. In all these cases, the trust mark schemes in effect in the EU today are more likely to become followers, once the new provisions have been adopted, rather than early-adopters, thus depriving EU data protection from potentially useful case studies. However, it should be noted, at the time of writing, that the GDPR wording is not yet finalised, and seal providers might be excused in demonstrating caution while adapting the set of rules applicable to their already operational schemes; after all, the two-year lead time afforded to them by the GDPR is expected to provide adequate time for any necessary adaptations and amendments.

On the other hand, the second point of convergence regarding EU-based schemes refers to their close adherence to the Data Protection Directive¹¹⁶ standards. Although levels of adherence may differ (at the top are the DPA-sponsored schemes in France and Germany such as the CNIL label and EuroPriSe), the fact-finding exercise has revealed that practically all EU-based schemes apply rigorously the EU Data Protection Directive provisions. This is not a self-evident fact, given that a few of such schemes are run by for-profits who would otherwise be bound to adopt a more flexible approach. Nevertheless, this has not been the case and EU data protection rules seem to have found their way into the relevant schemes. Here, an added value is met in terms of implementation: seal schemes provide a practical and accessible way for seal issuers to feel confident that their subscribers' actual business practices adhere to the law, and for individuals/consumers to trust providers of products or services.

A third point of convergence is found at a higher level; most analysed schemes appreciate and incorporate in their standards or criteria the basic data protection principles: fair and lawful acquisition and processing of data, processing for a declared purpose and for a limited amount of time to serve such purpose, etc. These principles are found both in the Data Protection Directive and outside the EU, most likely in the OECD Guidelines. Due to their ubiquity, the basic data protection principles are incorporated in some form or other in practically all schemes examined in this analysis, regardless of whether they are based in or outside the EU.

As far as points of divergence are concerned, the main finding refers to the fragmentation of all relevant efforts. Regardless of whether they are based in the EU or in third countries, the analysed schemes appear to constitute self-sufficient systems, with little concern for co-operation or much less mutual recognition. This patchwork of schemes could partly be attributed to the lack of common origins; their issuing organisations vary from data protection authorities themselves to for-profit organisations who offer to prepare, against a fee, a privacy policy if the one already adopted is found lacking. Obviously, the different regulatory environments within which they operate play a major role as well: the schemes analysed represent a diverse geographical coverage - the EU, USA, Japan and Canada – all of which apply largely different data protection systems in their respective jurisdictions.

An unsettling finding relates to the fragmentary nature of the European privacy seals landscape. While several schemes have been identified in certain Member States such as Germany or Spain, no noted attempts for mutual recognition and/or co-operation are evident. On the contrary, attempts have been noted to create local subsidiaries of Member State schemes, with moderate success, rather than co-operate with a local provider, who is already established. One of the Advisory Board members suggests that this lack of co-operation

¹¹⁶ European Parliament and the Council, Directive 95/46/EC 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, Brussels, 23 Nov 1995, pp. 31-50.

between schemes existed because many data protection authorities felt that they had no legal basis in their respective national laws that allowed them to do so (i.e., any new EU-wide scheme under the GDPR should provide a clear basis for that).

Apart from the fragmentation finding that practically affects all operational aspects of certification schemes in place today, a special note ought to be made with regard to the different legal environments that each scheme tries to accommodate. Many certification schemes are national in nature and are therefore guided to local rules and regulations: USA-based schemes apply privacy protection provisions, while EU trust mark schemes are data protection oriented. Although this assertion has already been made above, here it serves the purpose of demonstrating the grave differences among national schemes. This “agreement to be different” appears well-established within the schemes analysed.

8 BENEFICIARIES OF PRIVACY SEALS

First, this section identifies the beneficiaries of privacy seals and the benefits derived from privacy seals. Next, it identifies the impacts of privacy seal schemes on the beneficiaries. This is done with a view to improving the policy-making impact of the overall study.

8.1 BENEFICIARIES AND BENEFITS

For the purposes of this report, a beneficiary is any person or entity that benefits from the implementation and use of privacy seal schemes. These benefits may be monetary or non-monetary. They may be tangible (e.g., profits) or intangible (e.g., reputational advantage).

Based on the analysis of the 25 schemes, this section identifies and makes a broad analysis of the different, possible beneficiaries of privacy seal schemes. It examines this in terms of different stakeholders such as government (i.e., regulators, policy-makers, other public bodies), industry (sub-categorised under seal issuers, large buyers of privacy seals, SME buyers, third parties, industry associations), privacy and data protection organisations, consumers, individuals and society. These stakeholder groups are highly relevant for the implementation of future privacy seal options.

8.1.1 Government

This section focuses on government stakeholders such as policy makers, regulators and other public bodies.

8.1.1.1 Policy makers

Policy makers are responsible for determining and influencing privacy and data protection policy and practices at the European, national or local level. They operate in an environment of resource constraints (human and financial) and inflexibility. Their ability to influence and protect privacy and data protection interests is also dependant on other competing public priorities (that have to address a variety of needs) and public sector budgets. Policy making can also be a long, drawn-out process, subject to vetting, voting and rule-making, all of which take a significant amount of time. All this disadvantages policy makers in their efforts to optimise privacy and data protection in society.

Privacy seal schemes are more flexible and might have the capacity to assure privacy and data protection much more quickly and flexibly. These schemes can complement and fill the gaps in privacy and data protection policy making efforts. However, there may be a disincentive for scheme members to adopt constraints on their behaviour that go beyond what is required of the law.

The privacy accountability and compliance objectives of privacy and data protection policy can be served by an efficient and effective privacy certification scheme.

8.1.1.2 Regulators

Privacy and data protection regulators aim to “strike a balance between the rights of individuals to privacy and the ability of organisations to use data for the purposes of their business”.¹¹⁷

A study highlights how regulators have a stereotypical view that “smaller businesses seek not to comply with legislation” and conversely many businesses stereotype regulators as “strict enforcers” leading to a lack of trust and antagonism between the two.¹¹⁸ Privacy seal schemes can help regulators and businesses approach privacy and data protection compliance in a more collaborative and engaging manner.

Privacy and data protection regulators aim to produce certain outcomes, for instance, to ensure that privacy of individuals and personal information is properly and adequately protected. However, regulation and regulatory tools often have design flaws and inefficiencies that constrain regulators in their intent and ability to achieve this objective. Often regulation (and regulators) are criticised for lacking local knowledge and being out of touch with ground realities that affect the operation of regulation in practice. Further, though regulation might seem to be “politically attractive”, it has its downsides – e.g., over regulation, compliance and cost burdens.

Privacy seals may bring the following types of benefits to regulators: one, by providing privacy and data protection guarantees they undertake some of the objectives that privacy and data protection regulators try to achieve. Two, privacy seals create privacy accountability in a more visible and clear form that can be easily recognised and understood by individuals. This brings an indirect benefit to the regulator. Three, privacy seal issuers deal with privacy and data protection disputes and complaints that would otherwise burden regulators. Most privacy seal schemes require members to resolve disputes themselves, failing which they might resolve the matter themselves or refer it to an independent party for adjudication – this cuts down on the regulation and enforcement burden. Four, privacy seal schemes create an “additional level of oversight” – a view supported by the Smart Grid Privacy Seal scheme.¹¹⁹ On the other hand, regulators might see privacy seal schemes as competitors – who act in a manner that bypasses their regulatory role; this would impact the nature and level of any benefits.

¹¹⁷ Out-Law, “Data protection”, *Out-Law.com*, February 2008. <http://www.out-law.com/page-413>

¹¹⁸ Atherton, Andrew, Kirk Frith, Liz Price, Manny Gatt and David Rae, “The ‘Problem’ with Regulation: Systemic Constraints to Effective Implementation of New Legislation”, Institute for Small Business & Entrepreneurship, 5-7 November 2008. <http://www.isbe.org.uk/content/assets/BP08-AndrewAtherton.pdf>

¹¹⁹ TRUSTed Smart Grid. <http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-smart-grid>

8.1.1.3 Other public bodies

Administrative agencies also benefit from the implementation and use of privacy seal schemes. For instance, a privacy-certified business is better able to demonstrate compliance with privacy and data protection to an administrative agency procuring its services or evaluating its credentials for procuring its products and services. An administrative agency or other public body might also sub-contract out its services – for instance, a local authority might engage a company to manage its website which receives personal data from users; availing of a privacy-certified company might be a better alternative and a safer option than using a non-certified company and protect the agency from subsequent liabilities against actions by the sub-contractor. Thus, it may also create a privacy accountability benefit for public bodies.

8.1.2 Industry

The use of privacy seals is beneficial to industry. This has specifically been the case for the information technology industry. Through the use of privacy seals, a particular industry can demonstrate its good faith intention and efforts to self-regulate to alleviate privacy and data protection concerns and demonstrate compliance with industry best practice or regulatory requirements. The industry may thereby succeed in creating confidence and trust in itself.¹²⁰ Societal and regulatory stakeholders may view an industry making such efforts more favourably than one that does not use certification schemes.

An industry that advocates, facilitates and provides incentives for the use of privacy seals gains a market advantage, supporting trade and the growth of that industry.

In this part, we first look at privacy seal issuers. Next, we study buyers of privacy seals; these are separately classified into categories of large enterprises and SMEs (this distinction is crucial in understanding the differences in benefits accruing to these entities). Following this, we study third parties and industry associations.

8.1.2.1 Issuers of privacy seals

The prime beneficiaries of privacy seal schemes are privacy certifiers or seal issuers. Privacy certification is a profitable business. TRUSTe Inc. began as a non-profit organisation but converted to a for-profit company in 2008 (apparently to permit it “to make additional investments in our products to address the rapid adoption of new online technologies”). At inception, TRUSTe offered one privacy seal program. Since then, it has significantly expanded its privacy certification portfolio to include a wide range of privacy certifications for customers (e.g., TRUSTe Web privacy certification, EU Safe Harbor Certification Seal Program, Children's Privacy Seal, Email privacy certification, TRUSTed Downloads seal, TRUSTed Smart Grid Privacy Program, TRUSTed Cloud Data Privacy Certification program, TRUSTe-Promontory Binding Corporate Rules (BCR) Management Program and TRUSTe data collection certification. TRUSTe has more than 5,000 clients including Apple, Disney,

¹²⁰ EuroPriSe acknowledges this on its website. EuroPriSe, “Our Vision”. <https://www.european-privacy-seal.eu/about-europriSe/vision>

eBay, Facebook,¹²¹ Forbes, HP and Microsoft. This shows that privacy certification is a profitable business and that certification providers consider it a worthwhile investment.

Privacy certification is also advantageous for a seal issuer in terms of boosting its reputation. This brings an advantage to the organisation particularly if it offers other products and services in addition to its privacy certification schemes. TRUSTe, for example, in addition to providing privacy certification solutions, also markets the Website Monitoring Service¹²². Comodo CA Limited which offers trust certification (Comodo Corner of Trust and Comodo Standard TrustLogo) offers Internet security software solutions, PC support and maintenance, e-mail security, back-up and online storage solutions for the home, e-commerce and business solutions such as SSL (Secure Socket Layer) certificates, e-mail certificates, PCI (Payment Card Industry) compliance, PKI management and PC support.¹²³ Gigya Inc. (which offers SocialPrivacy™ Certification) offers social infrastructure for business (user management 360, social plug-ins and gamification).¹²⁴ Privacy Vaults Online Inc (which offers the PRIVO Privacy certified seal) sells products and services such as COPPA (the Children's Online Privacy Protection Act of 1998) Consulting, Strategy Assessment, PrivoLock™, private workshops and training, Global Kid ID Network and public speaking and seminar talks.¹²⁵

8.1.2.2 Privacy seal buyers – large enterprises

Large enterprises benefit in a number of ways from using privacy and data protection certification schemes. First, a privacy or data protection seal provides such enterprises with a visible means of demonstrating to their customers or users that they respect and fulfil *some* privacy or data protection standards or obligations. For instance, Microsoft believes its TRUSTe's Privacy Seal signifies that its “privacy statement and our practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability and choice regarding the collection and use of your personal information”.¹²⁶

To illustrate, a vast number of applications of Nintendo of America Inc. have ESRB Privacy Online certification.¹²⁷ Nintendo believes that this voluntary privacy initiative helps it protect its consumers and users privacy.¹²⁸ British Marks & Spencer is an ISIS (Trusted Shops) accredited retailer and marksandspencer.com is verified as an ISIS compliant website.¹²⁹ Apple, Inc, Lenovo¹³⁰ and IBM¹³¹ are TRUSTe's Privacy certified and display the TRUSTe privacy seal.¹³²

¹²¹ One of Facebook's investors (Accel Partners) is also an investor in TRUSTe. See Rao, Leena, “Baseline, Accel put \$15M in online Privacy Certification Company TRUSTe”, *Crunchbase*, 23 Jan 2012. <http://techcrunch.com/2012/01/23/baseline-accel-put-15m-in-online-privacy-certification-company-truste/>

¹²² TRUSTe, “Products and services”. <http://www.truste.com/products-and-services/>

¹²³ Comodo. <http://www.comodo.com/>

¹²⁴ Gigya Inc., “Products”. <http://www.gigya.com/products/>

¹²⁵ Privacy Vaults Online, “PRIVO's offerings”. http://www.privo.com/products_and_services.htm

¹²⁶ Microsoft Inc., “Microsoft Online Privacy Statement”. <http://privacy.microsoft.com/en-gb/fullnotice.aspx#ERDACC>

¹²⁷ See full list at ESRB, <http://www.esrb.org/privacy/sites.jsp>

¹²⁸ Nintendo Inc., <http://www.nintendo.com/corp/privacy.jsp>

¹²⁹ Marks & Spencer, “Privacy Policy”. <http://help.marksandspencer.com/faqs/company-website/privacy-policy>

¹³⁰ Lenovo. <http://www.lenovo.com/privacy/details/us/en/>

¹³¹ IBM. <http://www.ibm.com/privacy/details/uk/en/>

¹³² Apple Inc., Privacy. <http://www.apple.com/uk/privacy/>

An examination of some websites (and privacy policies) of major companies and organisations such as AXA, Vodafone, Zurich Insurance plc did not reveal the presence of privacy or data protection seals. This might be attributable to the fact that large enterprises have the propensity and ability to bank on their established reputation and use that to their advantage – perhaps the underlying assumption is that customers of large enterprises are more relaxed and less concerned about the ability of a large enterprise to protect their privacy and personal data.

However, given the recent privacy and data protection problems (particularly breaches involving personal data) that impact large enterprises, privacy certification (particularly certification that evaluates both privacy and security aspects) might provide an enterprise with an added layer of safety and compliance benefit, enabling the enterprise to identify and mitigate privacy risks and threats in a timely fashion and on a regular basis.¹³³ According to the UK Information Commissioner’s Office (ICO), “large private sector companies are lagging behind the public sector on their knowledge of data protection”, privacy certification enables such companies to become more aware of their privacy and data protection responsibilities.¹³⁴

8.1.2.3 Privacy seal buyers – small and medium enterprises

As compared to large enterprises and organisations, small and medium enterprises (SMEs) benefit more greatly from privacy certification. This is particularly if the enterprises are “lesser known” – it is argued that their consumers or users may need a greater or better and more concrete form of reassurance than if they were using the services of a large well known enterprise or organisation whose claims they might be better predisposed to take at face value.¹³⁵

Privacy or data protection seals help SMEs provide customers and users with a visible and defined proof of their commitment to privacy and data protection. They provide SMEs with a reputational advantage – privacy certified businesses might present a more credible image to a prospective customer or client as compared to a business that does not avail of such mechanisms.

Privacy seals also give SMEs a competitive advantage if they are able to draw and retain business on the basis of their privacy certification. This will ultimately impact their profits. In Schleswig-Holstein, Germany, the law permits public bodies of the State to give preference in procurement to IT products and services that are certified as complying with local data protection law.¹³⁶ This is an important aspect that should be considered at the EU level and in any new EU-wide proposed scheme.

¹³³ Navigant Consulting Inc., *Information Security & Data Breach Report, June 2012 Update*. http://www.navigant.com/insights/library/disputes_and_investigations/2012/information_security_data_breach_report_april_2012/

¹³⁴ ICO, “Big businesses lagging behind public sector on data protection awareness”, Press release, 5 November 2010. http://www.ico.org.uk/~/-/media/documents/pressreleases/2010/annual_track_2010_05112010.ashx

¹³⁵ Cline, Jay, “Web site privacy seals: Are they worth it?”, *Computerworld*, 8 May 2003. http://www.computerworld.com/s/article/81041/Web_site_privacy_seals_Are_they_worth_it

¹³⁶ See Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

<https://www.datenschutzzentrum.de/guetesiegel/index.htm>.

English information: https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm

Privacy seals enable SMEs (where required by law) to comply with regulations through the use of third party privacy certification. On their own and given their limited resources and expertise, SMEs might find it hard to determine and assess compliance with required or best practice standards.¹³⁷ Privacy seals fill this gap. For instance, the TRUSTe EU Safe Harbor Certification Seal Program permits US companies to demonstrate their compliance with the Safe Harbor Framework and the requirements of the EU Data Protection Directive (95/46/EC).¹³⁸

8.1.2.4 Third parties (e.g. independent evaluators, auditors)

Some privacy certification schemes mandate the use of services of independent evaluators or auditors. For instance, in the EuroPriSe scheme,¹³⁹ a seal applicant's products and services are evaluated by legal and technical experts according to evaluation criteria specific to the intended usage, legal framework and technical environment of the product. These legal and technical experts (called evaluators in the EuroPriSe scheme) benefit in two ways: one, they receive fees from clients for the evaluations, and two, from continually updating their privacy knowledge (according to EuroPriSe, "continuing privacy education is a mandatory requirement"¹⁴⁰).

8.1.2.5 Industry associations

Industry associations that issue privacy seals benefit from the advantages privacy certification brings to themselves and their members.

Industry associations such as the Market Research Society (MRS), which is responsible for the Fair Data scheme, not only financially benefit from subscriptions to their seals, but also gain publicity from the use of the seal on its members' websites and press releases highlighting the award of the seal.¹⁴¹ This helps raise its overall profile (alongside that of its members). The Cloud Security Alliance (CSA) which promotes "the use of best practices for providing security assurance within Cloud Computing" also derives a similar benefit.¹⁴² When the public or other stakeholders access the CSA STAR registry,¹⁴³ they might also be drawn to learn more about CSA, its membership, certification services and research. Thus, it can maximise its broader impact. The same would be true for other industry associations such as the Danish e-commerce Foundation (e-handelsfonden) administering the e-mark (e-mærket)¹⁴⁴ and Confianza Online (association representing the interactive advertising and e-commerce industries) which issues the Confianza Online trust mark.¹⁴⁵

The most illustrious case of the benefits privacy seal schemes can bring to a privacy association is the example TRUSTe. TRUSTe, initially launched as a non-profit industry

¹³⁷ Stanley, Martin, "Regulating Small Firms & Individuals", *Regulation*.
<http://www.regulation.org.uk/regsmes.pdf>

¹³⁸ TRUSTe, "EU Safe Harbor". <http://www.truste.com/products-and-services/enterprise-privacy/eu-safe-harbor-seal>

¹³⁹ EuroPriSe. <https://www.european-privacy-seal.eu/>

¹⁴⁰ EuroPriSe, "Privacy training". <https://www.european-privacy-seal.eu/index.html/expert-training/index.html>

¹⁴¹ Market Research Society. <http://www.mrs.org.uk/>

¹⁴² Cloud Security Alliance. <https://cloudsecurityalliance.org/>

¹⁴³ Cloud Security Alliance, "STAR registry entries". <https://cloudsecurityalliance.org/star/registry/>

¹⁴⁴ Emaerket. <https://www.emaerket.dk>

¹⁴⁵ Confianza Online. <http://www.confianzaonline.es>

association is now a “global data privacy management solutions provider” offering a wide range of solutions such as privacy by design consulting, privacy certifications, website monitoring tools and preference management platforms.¹⁴⁶

8.1.3 Privacy/data protection organisations

Some privacy organisations such as Privacy International have expressed reservations about “the value of ‘privacy seals’ which can often create an illusion of privacy protection without delivering anything additional to legal obligations”¹⁴⁷ Privacy and data protection organisations may not derive any direct benefit from privacy certification schemes (ideally, a privacy certified organisation might be able to capitalise on enhanced credibility). However, they do derive indirect benefits.

Privacy and data protection organisations can use the information generated by privacy seal schemes (for example, that contained in privacy seal registers) to keep a check on or verify certified entities (this benefit is also available to consumers/individuals but privacy organisations are in a better position to evaluate this information). For instance, DIGITTRADE High Security HDD HS256S (manufactured by DIGITTRADE GmbH) is certified by EuroPriSe.¹⁴⁸ Its certification report is available on the EuroPriSe website. A privacy organisation can use this report to check how the entity meets privacy and data protection requirements and verify this with actual practice or bring any issues/concerns to light.

8.1.4 Consumers

Consumers are a distinct category of privacy seals beneficiary. They benefit from the use and implementation of privacy and data protection seals. A privacy seal functions as a guarantee or assurance to a consumer that his or her privacy or personal data is or will be protected or treated in a fair and lawful manner. Privacy seals enhance the trust and confidence of consumers in a business or organisation with which they transact. Privacy seals enable consumers to save time and make quick decisions about whether a business or organisation is trustworthy. Privacy seals also help consumers understand privacy and data protection in a simple and user-friendly manner (compared to lengthy, non-user friendly privacy policies).

Some privacy seals bring special benefits to a specific type of consumer. For instance, the ESRB Kids Privacy Certified seal certifies compliance with requirements of the Children’s Online Privacy Protection Rule (16 C.F.R. Part 312) and enables parents, guardians and children to determine that children’s personal data is treated appropriately by certified entities.¹⁴⁹ PRIVO Privacy Certified (privacy seal focused upon websites collecting and processing information about children, and particularly children under the age of 13) benefits

¹⁴⁶ TRUSTe. <http://www.truste.com/about-TRUSTe/>

¹⁴⁷ Privacy International, “Response to the 2011 European Commission Consultation on Privacy”, 2011. <https://www.privacyinternational.org/reports/response-to-the-2011-european-commission-consultation-on-privacy/22-the-internal-market>. Privacy International questions the “value of privacy seals operated by for-profit companies when the profits of the seal program are wholly dependent on the revenues from seal holders”.

¹⁴⁸ EuroPriSe, “Register of Awarded Seals”. <https://www.european-privacy-seal.eu/awarded-seals>

¹⁴⁹ ESRB, “ESRB Privacy Certified Seals”. http://www.esrb.org/privacy/prog_req.jsp

children, parents and guardians.¹⁵⁰ Gigya's SocialPrivacy™ Certification benefits users of social websites, users of mobile applications.¹⁵¹

Good privacy seal schemes provide consumers with tangible and easily accessible privacy redress mechanisms. Most schemes enable consumers (or users of certified products and services) to contact them through e-mail, post or even consumer hotlines (e.g., ESRB). Confianza Online also provides “online consumers and businesses with a quick, inexpensive, and effective extrajudicial mechanism for solving disputes beyond the current fragmentary legislation of global regulations”.¹⁵² Privacy seal schemes such as ESRB act as mediators between member companies and complainants.¹⁵³ Some scheme operators such as the TÜViT provide detailed guidance on complaints-handling procedure, mandating that scheme members “record all complaints” and “immediately take necessary counter measures imposed by the complaints” and inform the certification body so that it can “judge about possible implications on the certification statement”.¹⁵⁴

8.1.5 Individuals

Individuals, as data subjects, benefit from the privacy and data protection assurance that privacy seals may provide. Privacy seal schemes aim to facilitate respect for an individual's privacy and personal information. For instance, the BBB Code of Business Practices specifies that accredited businesses must “protect any data collected against mishandling and fraud, collect personal information only as needed, and respect the preferences of customers regarding the use of their information”.¹⁵⁵ The Cloud Security Alliance STAR scheme aims to provide data subjects with data security, access to data and data breach notifications. The CNIL label for products or procedures intends to protect individuals in respect of processing of personal data, once it has recognised them to be in conformity with the provisions of the Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended).¹⁵⁶

Individuals benefit from the increased trust and confidence privacy seals aim to provide and from how privacy certification schemes and any discussion related to them brings about greater privacy and data protection awareness. Privacy certification schemes also provide individuals with tangible and easily accessible privacy redress mechanisms.

8.1.6 Society

Privacy certification is beneficial to society. Societal values are protected when privacy certification schemes encourage and facilitate good privacy practices. Society benefits through increased participation of individuals in online commercial and social activities.

¹⁵⁰ PRIVO. <http://www.privo.com/index.htm>

¹⁵¹ Gigya Inc., “Social privacy”. <http://www.gigya.com/social-privacy/>

¹⁵² Confianza Online. <http://www.confianzaonline.es>

¹⁵³ ESRB, <http://www.esrb.org/>

¹⁵⁴ TÜViT, *Certification Conditions for Test Mark Usage of the Certification Body TÜV Informationstechnik GmbH*, version 2009.

¹⁵⁵ BBB, “Code of Business Practices”. <http://www.bbb.org/us/bbb-accreditation-standards>

¹⁵⁶ CNIL, “CNIL Label”. <http://www.cnil.fr/linstitution/labels-cnil/>

The following table presents a beneficiaries-benefits summary and helps assess the benefits of privacy seals in relation to the various beneficiaries based preceding analysis:

BENEFITS	GOVERNMENT			INDUSTRY					PRIVACY ORGANISATIONS	CONSUMERS	INDIVIDUALS	SOCIETY
	Policy maker	Regulator	Other public body	Issuers of privacy seals	Privacy seal buyer - Large	Privacy seal buyer - SME	Third parties (e.g. auditors, third party verifiers)	Industry associations				
Support in generating privacy and data protection accountability/oversight	•	•	•						•		•	•
Privacy/data protection assurance/guarantee		•	•									•
Reduction in regulatory and enforcement burden	•	•										•
Enhance trust and confidence					•	•		•	•	•	•	•
Reputational advantage				•	•	•	•					
Competitive advantage				•	•	•						
Market advantage				•	•	•						
Boost trade and commerce				•	•	•	•	•				•
Increase in profits				•	•	•		•				
Drive industrial growth					•	•						•
Greater privacy information and awareness									•	•	•	•
Proof of fulfilment of privacy/data protection obligations					•	•						•
Implementation and maintenance of data protection measures					•	•						•
Easily able to see and verify privacy commitments									•	•	•	•
Quick and accessible privacy/data protection disputes redressal										•	•	•

Table 25: Beneficiaries-benefits summary

8.2 IMPACTS ON BENEFICIARIES

This section will briefly assess the impact of privacy seals in relation to the various beneficiaries. It will assess the propensity of organisations to subscribe to a privacy seal to improve the relationships with other stakeholders and customers and draw some initial conclusions about the complexity, burdens and overall impacts of a privacy seal from different perspectives. Based on the literature review and study of the individual privacy seal schemes, we have identified the following:

IMPACT	GOVERNMENT			INDUSTRY					PRIVACY ORGANISATIONS	CONSUMERS	INDIVIDUALS	SOCIETY
	Policy maker	Regulator	Other public body	Issuers of privacy seals	Privacy seal buyer - Large Co.	Privacy seal buyer - SME	Third parties (e.g. auditors, third party verifiers)	Industry associations				
Policy making/regulatory costs	•	•										
Design costs				•								
Cost of seal (certification & evaluation fees)					•	•				•		
Scheme administration costs				•								
Certification compliance costs					•	•						
Training costs				•	•	•	•					
Human resource cost				•	•	•						
Accreditation costs				•								
Regulatory approval costs				•								
Disclosure of personal information/false sense of privacy security										•	•	•

Table 26: Beneficiaries and impact

Policy-making/regulatory costs

Policy-making and regulatory costs refer to the costs associated with policy making, legislation and rule making. These impact policy makers and regulators.

Design costs

Design costs are largely borne by the certification scheme owner or operator.

Cost of seal

The cost of the seal (certification and evaluation fees) impacts subscribers to the schemes – these maybe large enterprises, small and medium enterprises or other organisations seeking privacy certification.

Seal administration costs

The privacy certification scheme administrator or operator bears the costs of administering the scheme.

Certification compliance costs

Certification scheme subscribers are faced with the costs of meeting the certification criteria requirements.

Training costs

There are different types of training costs. Privacy seal issuers may have to train personnel to administer the scheme, deal with complaints, and on privacy and data protection policy and legal aspects. Seal subscribers (of all types) may have to incur training costs; enterprises may have to train their employees to adhere to subscribed standards and train personnel to ensure compliance to subscribed standards. Third parties such as independent auditors and evaluators may incur costs associated with familiarisation with the Scheme's criteria and keeping abreast of privacy and data protection law and policy.

Human resource costs

Certification scheme operators have to invest in human resources to manage the scheme. Seal subscribers may have to designate one or more persons in the enterprise to check compliance with subscribed standards and manage its scheme related obligations.

Accreditation costs

Some certification schemes are accredited by other certification (industry or regulatory bodies).

Regulatory approval costs

Some certification scheme operators might incur these if they need to get approval from regulatory bodies.

Disclosure of personal information/false sense of privacy security

Privacy seal schemes, in some form or other, may indirectly promote a greater disclosure of personal information. For example, a user seeing a privacy seal he recognises on a website might trust that website and be more willing to disclose personal information to that website during his or her interactions with it as the website has demonstrated its credibility through the display of the seal. This is an important effect. This is because privacy seals when used thus might prompt privacy invasive websites and organisations to employ privacy seals as a means of gaining public credibility and as a front to shield their problematic privacy and data protection practices.

Privacy seals might also have the impact of lulling consumers, individuals (and society) into a false sense of *privacy security*. Consumers or individuals may begin to place too much reliance on third parties such as certified websites and certification authorities to protect their privacy or ensure that their personal data is adequately protected. While some certifiers may set and enforce high standards, our research has found that these differ widely across existing schemes, and consumers or individuals could be at risk when relying on certain seals or even duped by counterfeit seals.

9 CONCLUSIONS

The report comprehensively inventoried and analysed 25 privacy and related certification schemes in Europe and at the international level.

Key findings

The privacy seals market place is defined by heterogeneity. Whilst we can identify a relatively small number of ways in which seal schemes function, there is a large degree of variation around these core functional models. These variations can have significant implications for the claims that a seal scheme is legitimately able to make. In addition to this, the level of variation amongst seals likely impacts upon the effectiveness of seals. An individual (or organisation) cannot generalise about a seal scheme from their knowledge of other seal schemes (if any). It is a possibility that more niche seals will emerge, which will increase the level of variation further. Privacy seal schemes face a challenge in making legitimate claims about complex behaviours and standards, and making these claims rapidly, transparently, accessibly and communicating these reassuringly.

One of the key results of our study relates to the privacy and data protection elements of analysed schemes; some schemes have extensive privacy and data protection elements, others have none or a bare minimum. The focus of schemes differs. The more legally aligned schemes have a national or regional scope and coverage potentially restricting their universal application. The level of guarantees made to data subjects also varies – some schemes specify these explicitly, while others make no mention of it at all. While most of the analysed schemes seem to follow a typical model, there are highly divergent certification practices. This has implications for seal audiences who may not be able to determine the nature and scope of the certification process or to make informed judgements about a scheme that forms the basis of a seal. To this extent, it will be important to distinguish best practice from common practice in any future privacy seal scheme. A good privacy seal scheme must make

specific, concrete certification of privacy and data protection behaviour. Blending these claims with other business practices may diminish the distinctiveness of a privacy seal offering (as evident in some of the analysed schemes).

While the objectives of the analysed schemes cluster around six categories (building confidence or trust, signalling compliance or accordance with a standard, signalling the presence of privacy measures, providing guarantees, increasing market transparency and resolving disputes), and though there is some evidence of schemes achieving a certain measure of success (as in the case of profitable and expanding schemes such as TRUSTe), in actual practice, it is difficult to gauge the actual achievements of most of the objectives.

EU-based schemes display some key differences in comparison to their US-based or global counterparts. Europe has schemes administered by data protection agencies. The analysis also shows that European schemes are more likely to be aligned with legal standards for privacy and data protection, to make guarantees of compliance with such standards and requirements and less likely to have abstract guarantees on data subject rights. Non-EU schemes do not generally meet the legally-binding standards of EU data protection legislation.

In general, compliance with privacy and data protection law is a challenge for organisations. The GDPR imposes a high legal standard for privacy and data protection. Though the analysed EU-based certification schemes tend to approximate as best as possible the proposed GDPR requirements, unless guided effectively on how to concretely incorporate the GDPR requirements as their standards or criteria, they might fall short of what they can actually deliver through their schemes. For the non-EU based schemes, the GDPR criteria may be less relevant (attributable to different industry and regulatory environments within which they operate). Non-EU based schemes could adopt the GDPR criteria as this would give them a good standing and even form the basis for mutual recognition efforts if their subscribers engage with European consumers and data subjects.

Amongst the EU-based schemes, we find there is a lack of public discussion and preparation in relation to the new GDPR requirements (such as rights of data portability, right to be forgotten, data protection impact assessments, the principle of accountability and the special protection afforded to minors). EU-based schemes are also largely national in scope – while several schemes were identified in certain Member States such as Germany or Spain, no noted attempts for mutual recognition and co-operation are evident. This absence of harmonisation amongst EU-based seals puts them at a disadvantage in comparison to other international schemes that are able to cover a wider audience. EU citizens are exposed to a very wide variety of seal schemes in their use of the Internet; however, only a small sub-set of these schemes signal compliance with EU privacy and data protection law.

There are various beneficiaries of privacy seals: policy-makers, regulators, other public bodies, scheme operators, subscribers (of all types, large, medium and small), third parties (e.g., independent evaluators, auditors), industry associations, privacy and data protection organisations, consumers and individuals. On a broader front, privacy and data protection schemes benefit society. They encourage and facilitate good privacy and data protection practices and increase the participation of individuals in online commercial and social activities.

Privacy seal schemes can have various benefits (that are divergently applicable to beneficiaries): generation of privacy and data protection accountability and oversight,

provision of privacy assurances, reduction in the regulatory and enforcement burden, enhancement of trust and confidence, reputational, competitive and market advantages, increasing trade and commerce, driving industrial growth, generation of privacy awareness, helping prove fulfilment of privacy and data protection obligations, encouraging the implementation and maintenance of data protection measures, and presenting a quick and accessible means to determine and verify privacy and data protection commitments. These benefits were broadly supported by the stated objectives of many of the analysed seal schemes. These included abstract trust-building (encouraging a general sense of confidence, with trust strongly related to commercial opportunities for the certified entity), compliance signalling (with regard to laws or other standards), signalling data protection measures, the provision of binding guarantees, increasing market transparency and providing additional dispute resolution mechanisms. Each of these objectives can be understood as responding to particular problems of exercising trust online.

Privacy certification schemes also have an impact on their beneficiaries. This impact affects the propensity of organisations to subscribe to the scheme. The impact relates to various costs such as design costs, seal costs, seal administration costs, certification costs, certification compliance costs, human resource costs, accreditation costs, regulatory approval costs.

Required success factors for privacy seal schemes

One of the key factors that determine the extent to which a privacy certification scheme benefits individuals and citizens is how easy or difficult it is to break the link between the *signifier* (the presence of a seal on a website or entry in a register) and the *signified* (the particular privacy and data protection practices being certified). An effective seal must have a strong link between the two. Several factors identified in this study contribute towards weakening this link. The classical and linked seal models have weaker links between the *signifier* and *signified* than the hosted seal. This is because the website hosting the seal can potentially resist its revocation and continue to display a seal to which it is not entitled. Similarly, if a scheme fines a member who is in breach of its programme requirements rather than revokes the seal, then it becomes difficult for an end user to determine whether the seal represents a website in good standing with the programme requirements. The possibility of a negotiated relationship between seal provider and certified entity and too frequent changes to the programme requirements over time also undermine the link between the *signifier* and the *signified*, as a seal can signify different things on different websites, at different times. Finally a lack of information on what exactly the seal is supposed to signify is a concern. Too many of the analysed schemes were difficult to find, too abstract or had incomplete information accessible to the public. Given that the role of a seal is to signify something, it should be possible to determine what is being signified in a relatively easy and straightforward manner.

Transparency and openness of schemes is a necessity for ensuring that privacy seal schemes are not simply a front or means for an organisation to build and develop its profile and other supplementary activities (e.g., consulting). There is a need to eliminate this conflict of interest as it affects the credibility of the scheme.

Another key factor impacting the success of a privacy and data protection certification scheme is the certifier's reputation and ability to attract (and retain) subscribers. A certifier must be independent (financially and resources), capable of engendering trust from members and successfully able to implement and enforce the scheme. This may suggest the need for increased involvement from data protection authorities. Universality (ability to offer a more

widely applicable seal) of the scheme is another advantageous factor that might contribute to success of a scheme. Further, if SMEs are to gain the most from subscribing to these schemes, then certification schemes must find a way of catering to this beneficiary more effectively.

10 REFERENCES

Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 00062/10EN, WP 173, Brussels, 13 July 2010.

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

Associated Press, “Privacy-Assurance Seal Yanked”, *Wired.com*, 2 Sept 2005.

<http://www.wired.com/techbiz/media/news/2005/02/66557>

Atherton, Andrew, Kirk Frith, Liz Price, Manny Gatt and David Rae, “The ‘Problem’ with Regulation: Systemic Constraints to Effective Implementation of New Legislation”, Institute for Small Business & Entrepreneurship, 5-7 Nov 2008. <http://www.isbe.org.uk/content/assets/BP08-AndrewAtherton.pdf>

Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, MA, 2006.

Caslon Analytics, “Trust marks”. <http://www.caslon.com.au/trustmarksprofile.htm>

Cline, Jay, “Web site privacy seals: Are they worth it?” *Computerworld*, 8 May 2003.

http://www.computerworld.com/s/article/81041/Web_site_privacy_seals_Are_they_worth_it

Connolly, Chris, “Trust mark Schemes Struggle to Protect Privacy 2008”, Galexia, Version 1.0, 26 Sept 2008. http://www.galexia.com/public/research/assets/trust_marks_struggle_20080926

Consumer and Business Affairs Victoria, Department of Justice, “Web seals of approval”, Jan 2002.

<http://www.consumer.vic.gov.au/library/publications/resources-and-education/research/web-seals-of-approval-2002.pdf>

Cook, David, and Wenhong Luo, “The Role of Third-Party Seals in Building Trust Online”, *e-Service Journal*, Vol. 2, No. 3, Summer 2003, pp. 71-84.

Council of the European Union, Council conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting Brussels, 24 and 25 February 2011.

Databank Consulting. *Case Study: Euro-label*. Milan, 2004. http://ec.europa.eu/enterprise/archives/e-business-watch/studies/case_studies/documents/Case%20Studies%202004/CS_SR06_Retail_2-Euro-Label.pdf

Edelman, Benjamin, “Coupons.com and TRUSTe: Lots of Talk, Too Little Action”, 18 March 2008.

<http://www.benedelman.org/news/031808-1.html>

ESRB, “Websites certified by ESRB Privacy Online”. <http://www.esrb.org/privacy/sites.jsp>

European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM (2010) 609 final, Brussels, 4.11.2010.

http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

European Commission, Promoting Data Protection by Privacy Enhancing Technologies (PETs), Communication from the Commission to the European Parliament and the Council COM/2007/0228 final, Brussels, 2 May 2007.

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.

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.

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) Brussels, COM(2012) 11 final, 25.1.2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Parliament and the Council, Decision No 768/2008/EC of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, OJ L 218/82, 13 Aug 2008.

European Parliament and the Council, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002, p.0037-0047.

European Parliament and the Council, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, p. 54-63.

European Parliament and the Council, Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, p. 1-16.

European Parliament and the Council, Directive 95/46/EC 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, Official Journal L 281 , 23/11/1995 p. 0031 – 0050.

Goodin, Dan, “McAfee, Trust Guard certifications can make websites *less* safe”, *ARS Technica*, 6 Oct 2012. <http://arstechnica.com/security/2012/10/mcafee-trust-guard-certifications-can-make-websites-less-safe/>

Grabner-Kraeuter, S., “The Role of Consumers’ Trust in Online Shopping”, *Journal of Business Ethics*, Vol. 39, 2002, pp. 43-50.

Hansen, Marit, “Putting Privacy Pictograms into Practice - A European Perspective”, in Stefan Fischer, Erik Maehle and Rüdiger Reischuk (eds.), *Proceedings of GI Jahrestagung*, 2009, pp. 1703-1716.

Hu, Xiaorui, Zhangxi Lin and Han Zhang, “Myth or Reality: Effect of Trust-Promoting Seals in Electronic Markets”, in Otto Petrovic, Reinhard Posch and Franz Marhold (eds.), *Trust in a Networked Economy*, 2001, pp. 143-150.

Hui, Kai-Lung, Hock Hai Teo and Sang-Yong Tom Lee, “The Value of Privacy Assurance: An Exploratory Field Experiment”, *MIS Quarterly*, Vol. 31, Iss. 1, March 2007, pp 19-33.

Information Commissioner’s Office (ICO), “Big businesses lagging behind public sector on data protection awareness”, Press release, 5 November 2010.

http://www.ico.org.uk/~media/documents/pressreleases/2010/annual_track_2010_05112010.ashx

Kim, D.J., C. Steinfield and Y.-J. Ying-Ju Lai, “Revisiting the role of Web assurance seals in business-to-consumer electronic commerce”, *Decision Support Systems*, Vol. 44, No. 4, 2008, pp. 1000-1015.

LaRose, Robert, and Nora J. Rifon, “Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior”, *Journal of Consumer Affairs*, Vol. 41, Summer 2007, pp. 127–149.

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. 1009-1029.

Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended).<http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf>

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

Market Research Society, “Fair Data: Launch of personal data mark set to rebuild public trust”, 28 Jan 2013. <https://www.mrs.org.uk/article/item/696>

McAfee, “McAfee SECURE Website Certification Leads to Increased Sales”, *Data Sheet*. <http://www.mcafee.com/uk/resources/data-sheets/ds-mcafee-secure-for-websites.pdf>

McKnight, D. Harrison, Charles J. Kacmar and Vivek Choudhury, “Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initial trust in a web business”, *Electronic Markets*, Vol. 14, No. 3, 2004, pp. 252-266.

Milne, G.R., and M.J. Culnan, “Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don’t Read) Online Privacy Notices”, *Journal of Interactive Marketing*, Vol. 18, Issue 3, Summer 2004, pp. 15-29

Miyazaki, A., and S. Krishnamurthy, “Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions”, *Journal of Consumer Affairs*, Vol. 36, Issue 1, 2002, pp. 28-49.

Miyazaki, Anthony D., Sandeep Krishnamurthy and Debbie Roth, “Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions”, *Journal of Consumer Affairs*, Vol. 36, Summer 2002, pp. 28–49.

Moore, T., “Do consumers understand the role of privacy seals in e-commerce?”, *Communications of the ACM*, Vol. 48, No. 3, 2005, pp. 86-91.

Moore, Trevor T., and Gurpreet Dhillon, “Do privacy seals in e-commerce really work?”, *Communications of the ACM - Mobile computing opportunities and challenges*, Vol. 46, No. 12, December 2003, pp. 265-271.

Moulinos, K., J. Iliadis and V. Tsoumas, “Toward secure sealing of privacy policies”, *Information Management & Computer Security*, Vol. 12, No. 4, 2004, pp. 350-361.

Murdoch, Steven J. & Ross Anderson, “Verified by Visa and Mastercard SecureCode: Or, How Not to - Design Authentication”, in R. Sion (ed), *Financial Cryptography and Data Security*, LNCS 6052,

2010, pp. 336–342.; Ferguson, Rik, “Verified by Visa?”, *Countermeasures*, 01 Dec 2011. <http://countermeasures.trendmicro.eu/verified-by-visa/>

Navigant Consulting Inc., *Information Security & Data Breach Report, June 2012 Update*. http://www.navigant.com/insights/library/disputes_and_investigations/2012/information_security_data_breach_report_april_2012/

O’Connor, Peter, “An International Comparison of Approaches to Online Privacy Protection”, in Andrew J. Frew (ed.), *Information and Communication Technologies in Tourism 2005: Proceedings of the International Conference in Innsbruck, Austria*, Springer, Vienna, 2005, pp. 273-284.

Organisation for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980.

Out-Law, “Data protection”, *Out-Law.com*, February 2008. <http://www.out-law.com/page-413>

PCI Security Standards Council, PCI SSC Data Security Standards (PCI DSS). https://www.pcisecuritystandards.org/security_standards/

Privacy International, “Response to the 2011 European Commission Consultation on Privacy”, 2011. <https://www.privacyinternational.org/reports/response-to-the-2011-european-commission-consultation-on-privacy/22-the-internal-market>

Rhee, Joseph and Brian Ross, “Terror group gets ‘A’ rating from Better Business Bureau”, *ABC News*, 12 Nov 2010. <http://abcnews.go.com/Blotter/business-bureau-best-ratings-money-buy/story?id=12123843>

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.

Stanaland, Andrea J.S., May O. Lwin and Anthony D. Miyazaki, “Online Privacy Trust marks: Enhancing the Perceived Ethics of Digital Advertising”, *Journal of Advertising Research*, September 2011, pp. 511-523.

Stanley, Martin, “Regulating Small Firms & Individuals”, *Regulation*. <http://www.regulation.org.uk/regsmes.pdf>

Tan, Andrew, “Privacy seals”, ACC 626 Information System Assurance & Computer-Assisted Auditing 2011. <http://uwvisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Privacy%20Seals%20A%20Tan.pdf>

TNO and Intrasoft, *EU online Trust marks: Building Digital Confidence in Europe*, A study prepared for the European Commission DG Communications Networks, Content & Technology, Final report, SMART 2011/0022, 2012.

TRUSTe, “Cisco Systems, Inc.-case study”. <http://www.truste.com/customer-success/cisco-systems/>

TRUSTe, “Customers choose to do business with companies they trust”, <http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-websites>

TRUSTe, “Oracle- case study”. <http://www.truste.com/customer-success/oracle/>

Trzaskowski, Jan, “E-commerce trust marks in Europe – An overview and comparison of trust marks in the European Union, Iceland and Norway”, 2006.

TÜViT, *Certification Conditions for Test Mark Usage of the Certification Body TÜV Informationstechnik GmbH*, version 2009.

ValidSoft, “ValidSoft achieves unprecedented third European Privacy Seal”, *ValidSoft News*, 13 November 2012. <http://www.validsoft.com/news/validsoft-achieves-unprecedented-third-european-privacy-seal-news-23181314243>

Winston & Strawn LLP, “Biometrics: French officials warning”, *Briefing*, February 2007.

Zetter, Kim, “Hack obtains 9 bogus certificates for prominent websites; traced to Iran”, *Wired: Threat Level*, 23 March 2011. <http://www.wired.com/threatlevel/2011/03/comodo-compromise/>

11 ANNEX I – INDIVIDUAL PRIVACY SEAL PROFILES

This Annex presents the profiles for each of the inventoried privacy seals in the following format:

	General criteria for evaluation and comparison of privacy seals	Privacy seal X
1	Nature (privacy-oriented/general trust mark)	
2	Country	
3	Inception	
4	Issuing organisation	
5	Issuer type	
6	Target of scheme	
7	Number of certified entities	
8	Renewals	
9	Types of entities that can be certified	
10	Type of beneficiaries	
11	Objective of scheme	
12	Descriptive summary of scheme	
13	Unique selling point	
14	Privacy/data protection elements of the scheme	
15	Guarantees offered to the data subject	
16	Steps in the certification process	
17	Coverage of international transfers	
18	Costs (i.e., evaluation cost, certification cost)	
19	Validity	
20	Revocation mechanism	
21	Recognition	
22	Accredited experts and/or evaluation bodies	
23	Duration and scope of the certification process	
24	Number of certified experts and/or bodies	
25	Regulatory/ compliance standards	
26	Frequency and means of updates to scheme	
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	
28	Complaints mechanism	
29	Criticisms	
30	Links and references to the scheme	
31	Logo	
32	Website	


	General data protection regulation requirements	
33	Fair, lawful, transparent processing of personal data	
34	Data collection for specified, explicit and legitimate purposes	
35	Adequate, relevant and limited data collection	
36	Data accuracy	
37	Time and purpose restricted data retention	
38	Data is processed under the responsibility and liability of the controller	
39	Provision for parental consent based processing of personal data of a child below the age of 13	
40	Consent requirement for processing of special personal data	
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	
43	Existence of procedures and mechanisms for exercising the rights of the data subject	
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	
46	Provision for right of access for the data subject	
47	Provision for right to rectification	
48	Provision for right to be forgotten and to erasure	
49	Provision for right to data portability	
50	Provision for data subject's right to object	
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	
52	Rights in relation to automated processing	
53	Documentation requirements (Article 28)	
54	Implementing the data security requirements (Article 30)	
55	Notification of a personal data breach to the supervisory authority (Article 31)	
56	Communication of a personal data breach to the data subject (Article 32)	
57	Data protection impact assessment (Article 33)	
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Articles 34(1) and (2)	
59	Designation of a data protection officer (Article 35(1))	
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations (Article 22)	

Table 27: Collated scheme assessment table

11.1 BBB ACCREDITED BUSINESS SEAL

	General criteria for evaluation and comparison of privacy seals	BBB Accredited Business Seal
1	Nature	General
2	Country	USA
3	Inception	1999
4	Issuing organisation	BBBOnLine (Better Business Bureau)
5	Issuer type	Corporation of private business franchisees (subsidiary of the Council of BetterBureaus)
6	Target of scheme	Businesses based in the United States and Canada
7	Number of certified entities	145,700 websites accredited as meeting BBBOnLine standards (as at 2012)
8	Renewals	Not clear
9	Types of entities that can be certified	Businesses based in the United States and Canada
10	Type of beneficiaries	Primarily consumers in the US, Canada; certifying businesses.
11	Objective of scheme	To demonstrate that a “business meets accreditation standards which include a commitment to make a good faith effort to resolve any consumer complaints”. See website .
12	Descriptive summary of scheme	BBB accredited businesses’ pay fees for accreditation review/monitoring and for support of BBB services. BBB accreditation “does not mean that the business’ products or services have been evaluated or endorsed by the BBB or that BBB has made a determination as to the business’ product quality or competency in performing services”. See website .
13	Unique selling point	<ul style="list-style-type: none"> • Use of seal in traditional advertising media (newspapers, periodicals, billboards, posters, direct mail, flyers, yellow pages or other directory advertising, telephone, TV or radio spots, business cards, stationery, invoices, facsimile cover sheets and other business documents) and online advertising. • Seal as well as rating based assurance. See http://www.bbb.org/business-reviews/ratings/ • Searchable database
14	Privacy/data protection elements of the scheme	The BBB Code of Business Practices specifies that accredited businesses must “protect any data collected against mishandling and fraud, collect personal information only as needed, and respect the preferences of customers regarding the use of their information”.
15	Guarantees offered to the data subject	Respect of privacy, security for sensitive data, honouring of customer preferences.
16	Steps in the certification process	The accreditation process is aimed at determining if a business meets “truth in advertising guidelines”, discloses information about its business and policies, follows basic privacy and

		security practices and responds appropriately to problems. Businesses meeting BBB standards are presented to local Boards of Directors (or designees) for review and acceptance as a BBB Accredited Business. A BBB accredited business can display the BBB Accredited Business seal online following confirmation of their adherence to the BBB Code of Business Practices , including its online standard.
17	Coverage of international transfers	Not specified in respect of seal. BBB operates a separate EU Safe Harbor Privacy Dispute Resolution Program.
18	Costs (i.e., evaluation cost, certification cost)	Fees for Accredited BBB membership: \$379-\$1499 based on number of employees. Fee for non-profit organisations is \$235. [Annual fees for BBB EU Safe Harbor Privacy Dispute Resolution Program is based on total sales of applicant and range from \$300- \$7,000]
19	Validity	The term of the business's agreement with BBB begins when it is accepted by BBB and continues unless terminated by either party or for failure to pay annual fees.
20	Revocation mechanism	BBB may suspend and/or terminate its agreement with a business at any time if the business violates the terms of its agreement. On suspension or termination of the agreement the business must cease using the BBB seal. A business can ask for a review of the suspension under applicable procedures set forth in the BBB Bylaws. Unless the suspension is set aside, the suspension becomes final and the agreement is terminated.
21	Recognition	Nearly 400,000 local businesses in North America support the BBB. The BBB is a well-recognised entity. Its seal is also well recognised.
22	Accredited experts and/or evaluation bodies	113 independently incorporated local BBB organisations.
23	Duration and scope of the certification process	This is not clear. One firm reported the process took five months.
24	Number of certified experts and/or bodies	Not clear.
25	Regulatory/ compliance standards	Compliance with the BBB Code of Business Practices (BBB Accreditation Standards). A BBB accredited business must adhere to federal, state/provincial and local advertising laws. Businesses are also expected to "Businesses will make best efforts to comply with industry standards for the protection and proper disposal of all sensitive data, both online and offline.
26	Frequency and means of updates to scheme	None specified on website.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness)	Sound advertising, selling and customer service practices are encouraged to enhance customer trust and confidence in business.
28	Complaints mechanism	BBB accepts all types of complaints. The

		complaint is forwarded to the business within two business days and it is asked to respond within 14 days. If a response is not received, a second request is made. The complainant is You notified of the business's response when BBB receives it (or notifies the complainant that it has received no response). Complaints "are usually closed within 30 business days".
29	Criticisms	<ul style="list-style-type: none"> • Lack of neutrality (encourages and solicits money from businesses it monitors) • BBB's "too cozy" relationship with some of the businesses it claims to monitor (90% of BBB board members are reportedly corporate executives from industries that generate large numbers of BBB complaints) • BBB reliability reports are biased toward accredited businesses • Complaints are sometimes closed even when the consumer is greatly dissatisfied with the company's response.
30	Links and references to the scheme	<ul style="list-style-type: none"> • Hu, Xiaorui, Guohua Wu, Yuhong Wu, and Han Zhang, "The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective", <i>Decision Support Systems</i>, Vol. 48, No. 2, 2010, pp. 407-418. • Lacho, Kenneth J., "How a Better Business Bureau (BBB) can help BBB Accredited small business members," <i>Academy of Entrepreneurship</i>, Vol. 16, No. 1, 2010. • Fleming, Troy, "Pay for Play Scandal at the Better Business Bureau Leads to Consumer Mistrust of the Business Rating Organization", <i>Loyola Consumer Law Review</i> Vol. 23, 2010, pp. 445. • Hansen, Marit, "Putting privacy pictograms into practice- A European perspective," <i>GI Jahrestagung</i> 154, 2009, pp. 1703-1716. • Parmar, Neil, "Is the BBB Too Cozy With the Firms It Monitors?" <i>SmartMoney</i>, 24 September 2008.
31	Logo	
32	Website	http://www.bbb.org/online/
General data protection regulation requirements under Ch II and III		

33	Fair, lawful, transparent processing of personal data	The BBB Code of Business Practices requires members to “Protect any data collected against mishandling and fraud,” and respect the preferences of customers regarding the use of their information.
34	Data collection for specified, explicit and legitimate purposes	The BBB Code of Business Practices requires businesses to disclose on website what information they collect, with whom it is shared.
35	Adequate, relevant and limited data collection	Businesses should collect personal information only as needed.
36	Data accuracy	Businesses must inform data subjects about how data can be corrected.
37	Time and purpose restricted data retention	Not specified
38	Data is processed under the responsibility and liability of the controller	Maybe implicit. Not explicitly provided in its Code .
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not specified. BBB has a separate CARU Safe Harbor Program – see http://www.bbb.org/us/CARU/Safe-Harbor/ .
40	Consent requirement for processing of special personal data	Only calls for “respect the preferences of customers regarding the use of their information”.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	The BBB Code of Business Practices requires businesses to “Be Transparent” – i.e. openly identify the nature, location, and ownership of the business, and clearly disclose all policies, guarantees and procedures that bear on a customer’s decision to buy.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Requires businesses to disclose on website: what information they collect, with whom it is shared, how it can be corrected, how it is secured, how policy changes will be communicated, and how to address concerns over misuse of personal data.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Specified in BBB Code of Business Practices as a requirement.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	The BBB Code of Business Practices calls on businesses to specify on website how personal information can be corrected. The right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement not specified as such. Article 17 (right to be forgotten and to erasure) related action not specified in Code.
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation 	Requires businesses to disclose on website: information they collect, with whom it is shared, how it can be corrected, how it is secured, how policy changes will be communicated, and how to address concerns over misuse of personal data.


	reference to an adequacy decision by the Comm <ul style="list-style-type: none"> Any further information necessary to guarantee fair processing 	
46	Provision for right of access for the data subject	None specified in BBB Code of Business Practices .
47	Provision for right to rectification	Yes.
48	Provision for right to be forgotten and to erasure	None specified in BBB Code of Business Practices .
49	Provision for right to data portability	None specified in BBB Code of Business Practices .
50	Provision for data subject's right to object	No. Not very clear in this respect.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	None specified in BBB Code of Business Practices .
52	Rights in relation to automated processing	None specified in BBB Code of Business Practices .
53	Documentation requirements (Art 28)	None specified in BBB Code of Business Practices .
54	Implementing the data security requirements (Article 30)	The BBB Code of Business Practices specifies "Businesses that collect sensitive data online (credit card, bank account numbers, Social Security number, salary or other personal financial information, medical history or records, etc.) will ensure that it is transmitted via secure means. Businesses will make best efforts to comply with industry standards for the protection and proper disposal of all sensitive data, both online and offline".
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not specified in BBB Code of Business Practices .
56	Communication of a personal data breach to the data subject (Article 32)	Not specified in BBB Code of Business Practices .
57	Data protection impact assessment (Article 33)	Not specified in BBB Code of Business Practices .
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not specified in BBB Code of Business Practices .
59	Designation of a data protection officer (Article 35(1))	Not specified in BBB Code of Business Practices .
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	Not specified in BBB Code of Business Practices .

11.2 BUYSAFE GUARANTEED SHOPPING

	General criteria for evaluation and comparison of privacy seals	buySAFE Guaranteed Shopping
1	Nature	E-commerce guarantee scheme
2	Country	United States
3	Inception	buy SAFE Incorporated 2003 (active launch 2006)
4	Issuing organisation	buySAFE, Inc
5	Issuer type	Private company
6	Target of scheme	Businesses based in the United States
7	Number of certified entities	Over 5,000
8	Renewals	Unclear
9	Types of entities that can be certified	Online retailers
10	Type of beneficiaries	Online retailers, online consumers (international)
11	Objective of scheme	To address buyer confidence in online commerce by providing additional guarantees and bonds. Targeted at online transactions.
12	Descriptive summary of scheme	buySAFE allows online retailers to provide their customers with a third-party guarantee on their online shopping. The aim is to increase customer confidence in the retailer and the experience, and decrease concerns about information security, product authenticity and timely delivery, and thereby increase the volume of online sales. The buySAFE guarantee can either be provided for every transaction on an online store or can be provided as an option that the customer can purchase individually. The proposition to the retailer is that the increased profits from additional sales will cover the costs of the guarantee. The guarantee includes identity theft protection cover. buySAFE states that it conducts some inspection and verification of online merchants before it allows them to offer the guarantee. The scheme is primarily a form of additional insurance. The scheme does not make specific guarantees about the data protection or personal information handling policies of the websites to which it applies, but instead provides a dispute resolution and (limited) restitution mechanism for identity theft.

13	Unique selling point	<ul style="list-style-type: none"> • The scheme offers a mechanism for resolution in the event something goes wrong with the online transaction. • Guaranteed shopping experience, guarantee includes identity theft protection, purchase guarantee and lowest price guarantee • Two services (buySAFE Bonded which allows customers to buy guarantee with their purchase, is free to merchants; For buySafe Guarantee, which gives guarantee on all purchase, merchant pays percentage of sale to buySAFE).
14	Privacy/data protection elements of the scheme	<ul style="list-style-type: none"> • Identity theft protection for US customers. • Privacy and security policy on buySAFE website
15	Guarantees offered to the data subject	Live identity theft restoration services, and \$10,000 financial reimbursement for 30 days from the transaction.
16	Steps in the certification process	<p>Online application process initiated by online retailers wishing to use the guarantee scheme. Eligibility is based upon a track record of success, financial stability, and commitment to fulfilling promises made to buyers. buySafe requests information from the seller to verify their identity and financial stability, including a valid credit card, and basic information about the business (including total monthly sales, and how long the company has been selling online) and business owner. buySAFE claims to conduct a business inspection and identity verification check to determine if businesses qualify.</p> <p>buySAFE also states that it collects the following information about business:</p> <ol style="list-style-type: none"> 1. Information received on application or other forms 2. Information about business performance in its dealings with buySAFE, buyers, affiliates or others; 3. Information received from a consumer reporting agency, business credit bureaus and other authoritative sources; and 4. Information from publicly available online sources. <p>If accepted, a pricing model is determined or negotiated. (See 18 below).</p>
17	Coverage of international transfers	International sales (where buyer is not in the USA) can be covered by the guarantee scheme, but the scheme only currently applies to US retailers.
18	Costs (i.e., evaluation cost, certification cost)	The pricing scheme based upon sales volume and the merchant's additional profit from using the scheme. Example cost is 1% transaction fee on Overstock.com transactions in a partnered

		programme. In this example, where all transactions are guaranteed, buySAFE takes 1% from each transaction.
19	Validity	A 30 day free trial starts after the certification process, then ongoing, monthly or yearly payments. There is no information given on how regularly buySAFE updates its assessments of eligibility.
20	Revocation mechanism	Bonded retailers are required to allow buySAFE access to inspect their business at any time. Revocation of seal or guarantee service can happen at any time and without notice if the retailer fails to: keep information provided to buySAFE current; properly display the seal or promotional information; follow the dispute resolution procedure, standards or prohibited items, enable customers to purchase the bonding service or receive all the benefits of it, or if the merchant is no longer a member of good standing in their marketplace. buySAFE may also revoke the seal if they receive complaints about the merchant or merchants do not provide bond claims payment information with buySAFE. The revocation is supported by contract law.
21	Recognition	The buySafe website hosts a TRUSTe Privacy seal, and buySafe is recognised by the Better Business Bureau (BBB).
22	Accredited experts and/or evaluation bodies	None mentioned other than buySAFE and its insurance providers.
23	Duration and scope of the certification process	No information provided on the duration of the certification process, but it appears fairly rapid.
24	Number of certified experts and/or bodies	N/A
25	Regulatory/ compliance standards	buySAFE is governed by US law, and specifically by that of the state of Virginia.
26	Frequency and means of updates to scheme	No information provided on frequency of changes to the scheme. If scheme is thought of as a contractual relationship between buySAFE and each individual online retailer then terms could change rapidly. There is evidence to suggest that buySAFE uses a range of insurance and bond providers for different circumstances.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	<ul style="list-style-type: none"> • Accredited business with the Better Business Bureau (BBB). • TRUSTe Web Privacy seal • The programme has an associated browser plug in to support safe online shopping: http://download.cnet.com/buySafe-Shopping-Advisor-for-Internet-Explorer/3000-12512_4-10868212.html . • Dispute resolution service.
28	Complaints mechanism	For complaints related to buySAFE itself, communications are directed to customersupport@buySAFE.com
29	Criticisms	<ul style="list-style-type: none"> • Seven complaints with the Better Business Bureau over last three years (Five resolved

		with BBB assistance. In two cases, the BBB found that buySAFE had made a good faith effort to resolve the case, but the customer was unsatisfied.
30	Links and references to the scheme	<ul style="list-style-type: none"> Nichols, Shaun, “VeriSign and buySAFE team up on e-commerce security”, v3.co.uk, 5 Aug 2009. http://www.v3.co.uk/v3-uk/news/1949701/verisign-buysafe-team-commerce-security Wauters, Robin, “buySAFE Sues Google Over “Trusted Stores” Service, Fears Annihilation”, <i>TechCrunch</i>, 27 Dec 2011. http://techcrunch.com/2011/12/27/buysafe-sues-google-over-trusted-stores-service-fears-annihilation/
31	Logo	
32	Website	http://www.buysafe.com/index.html
	General data protection regulation requirements under Ch II and III	[Note: Most of the following material is taken from the buySAFE Privacy and Security Policy – buySAFE is incorporated under the legal jurisdiction of the state of the Virginia. Most of the information provided is orientated towards buySAFE’s own information practices, as the scheme does not make substantial claims about the information handling practices of its members, or place such requirements upon them.
33	Fair, lawful, transparent processing of personal data	The buySAFE scheme does not appear to guarantee the privacy and personal information handling related practices of merchants using the guarantee scheme.
34	Data collection for specified, explicit and legitimate purposes	buySAFE provides explanations of the data it collects and the purposes for this collection in its privacy policy and terms and conditions for merchants. It states “We collect information about you and/or your business in order to qualify the best merchants on the web. We verify your identity and we use the credit and business information we collect to determine whether you qualify as a buySAFE Merchant. Your contact information is used to explain our services, to send invoices, and to resolve problems related to consumer purchases that involve our services.”
35	Adequate, relevant and limited data collection	Information is provided in the Privacy and security policy on the broad types of data collected and purposes of collection. Regarding merchants using the scheme, it states: We collect information about you and/or your business from the following sources: <ol style="list-style-type: none"> Information we receive from you on our application or other forms; Information about your performance in your dealings with us, our buyers, our affiliates or others;

		<p>3. Information we receive from a consumer reporting agency, business credit bureaus and other authoritative sources; and</p> <p>4. Information from publicly available online sources.</p> <p>Customers' information collected includes non-personally identifying information such as IP addresses, browser types, domain names, time and date stamps, referring URLs, pages viewed, number of clicks, and other usage data. buySAFE uses this information to analyse trends, to track visitors' movement in the aggregate, and to gather general information about which pages are visited – all to improve buySAFE services. buySAFE collects personally identifiable information when a transaction occurs in order to issue its guarantee for the purchaser. If a buyer needs to check their benefits, make a claim, report a problem or to report a suspected misuse of the buySAFE Seal, then the buyer must register online and complete a Report a Problem Transaction Form. When filing a claim, we require that buyers provide their name, email address, city, state, country, postal code, name of the web site, URL, and a description of the issue they are reporting. buySAFE uses the information to investigate and resolve buyer benefit claims, including contacting claimants and merchants as necessary. BuySAFE may use the data in anonymized or aggregate form to provide and improve its services and to develop new services.</p>
36	Data accuracy	In relation to personal data held by the company –the buySAFE Privacy and security policy states, “If you believe that any information is incorrect, or would like to delete/deactivate your personally identifiable information, notify us immediately by either completing a "Contact Us" form or sending an email message to customersupport@buySAFE.com , and we will promptly correct erroneous information or discontinue your service.”
37	Time and purpose restricted data retention	Data is retained for the duration of the provision of service. The buySAFE Privacy and security policy states: “We will retain your information for as long as your account is active or as needed to provide you services. If you wish to cancel your account or request that we no longer use your information to provide you services contact us at customersupport@buySAFE.com . We will retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.”
38	Data is processed under the responsibility and liability of the controller	Contact details and address of the company are provided with the legal notices and in the contact information section of its website.
39	Provision for parental consent based	buySAFE appears to have no intent to process the

	processing of personal data of a child below the age of 13	personal data of children below the age of 13. The scheme makes no requirements regarding this on members. The buySAFE Privacy and security policy states, “buySAFE’s websites, products, and services are neither developed for, nor directed at, children (those under 18 years of age). If you believe your child has provided buySAFE with personally identifiable data, or registered at one of buySAFE’s websites, and you would like to have the data removed, please contact us”.
40	Consent requirement for processing of special personal data	Personal data of merchants and customers is processed. Consent appears to be based upon the merchant signing up to use the guarantee scheme, or a customer purchasing an additional guarantee. Consent appears presumed where a customer uses a website where buySAFE guarantees all transactions. In this context, information might be transmitted to buySAFE without explicit consent or intent of the data subject.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	buySAFE has a combined Privacy and security policy posted on its website, in a section of legal notices. It can be reached from the front page. This privacy policy primarily deals with information collected by the site, and
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	No particular information on the processing of information addressed specifically to a child.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	buySAFE’s privacy and security policy provides a number of mechanisms through which data subjects can correct inaccuracies in their information, or request that processing of their personal data be terminated (along with ending the provided service), but these are not expressed in terms of rights of the data subject. The guarantee scheme does not place equivalent obligations upon scheme members.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	buySAFE provides the following information under the heading of “Updating and Changing Personally Identifiable Information” in its Privacy and security policy : buySAFE provides you with access to your personally identifiable information in our database. You may view and in certain cases update your personally identifiable information (such as zip code, phone, email or postal address) by visiting My Account section of the service center on the buySAFE Web site, www.buySAFE.com . If you believe that any information is incorrect, or would like to delete/deactivate your personally identifiable information, notify us immediately by either completing a "Contact Us" form or sending an email message to customersupport@buySAFE.com , and we will promptly correct erroneous information or


		discontinue your service. This makes no relation to Articles 16 and 17.
45	<p>Provision of information to data subject:</p> <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation in reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	<p>In the context addressed by the buySAFE policies, the data subject is either the visitor to their website, an online merchant using the guarantee service, or a customer purchasing a guarantee through such a merchant. The information provided below refers to buySAFE's data processing.</p> <ul style="list-style-type: none"> • Postal address and email addresses are provided for customer support at buySAFE, but they are not specifically identified as the Data Controller. • No information on right to request access is provided. Information is provided on a procedure for rectification and erasure of data, but this is not identified as a legal right. • No information on supervisory authority and right to lodge complaint. • No information on transfers to third country or international organisation (company is located in a third country – the United States). The Privacy and security policy states that “Residents of the European Union and other non-US residents who visit or use our site or services understand and consent to the processing of personally identifiable information in the United States.” • The buySAFE Privacy and security policy states: Though we will at all times act in a way that respects your privacy, we may need to disclose personally identifiable information when required by law where we have a good-faith belief that such action is required by law, or to prevent or detect a fraud, security or technical issue, or to protect against imminent harm to the rights, property or safety of our users, buySAFE, or the public as required or permitted by law. • The buySAFE website suggests it will disclose information to financial institution partners, payment companies, bonding partners & vendors; third party web analytic companies (in non-personally identifiable form); as required by law, or in the case of a merger or acquisition.
46	Provision for right of access for the data subject	Not specified in the buySAFE Privacy and security policy .
47	Provision for right to rectification	Yes, see 36 above.
48	Provision for right to be forgotten and to erasure	No information given on right to be forgotten and to erasure.
49	Provision for right to data portability	No information given on data portability.
50	Provision for data subject's right to object	No information given on right to object
51	Right to object free of charge to the	No information given on direct marketing

	processing of their personal data in cases of direct marketing (explicit offering of right)	
52	Rights in relation to automated processing	No information given on rights relating to automated processing
53	Documentation requirements (Art 28)	No information provided.
54	Implementing the data security requirements (Article 30)	No evidence
55	Notification of a personal data breach to the supervisory authority (Article 31)	No information
56	Communication of a personal data breach to the data subject (Article 32)	No information
57	Data protection impact assessment (Article 33)	No evidence
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	No information
59	Designation of a data protection officer (Article 35(1))	Not named. No specific contact details provided.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	buySAFE, Inc. has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability and choice regarding the collection and use of your personally identifiable information.

11.3 CLOUD SECURITY ALLIANCE

	General criteria for evaluation and comparison of privacy seals	Cloud Security Alliance
1	Nature (privacy-oriented/general trust mark)	General (publicly accessible registry that documents the security controls provided by various cloud computing offerings). No certification seal/mark.
2	Country	USA
3	Inception	Q4 of 2011.
4	Issuing organisation	Cloud Security Alliance (CSA)
5	Issuer type	Non-profit, private sector association
6	Target of scheme	Cloud computing providers/ cloud consumers
7	Number of certified entities	29 entries on the registry.
8	Renewals	-
9	Types of entities that can be certified	Cloud computing providers
10	Type of beneficiaries	Cloud consumers/users
11	Objective of scheme	To allow potential cloud customers to review security practices of providers.
12	Descriptive summary of scheme	CSA STAR is a publicly accessible registry that documents the security controls provided by various cloud computing providers. It is based upon the CSA Governance, Risk, and Compliance (GRC) Stack , a collection of four integrated research projects that provide a framework for cloud-specific security controls, assessment, and greater automation and real-time GRC management. CSA STAR is open to all cloud providers, and allows them to submit self-assessment reports that document compliance to CSA published best practices. The searchable STAR registry allows potential cloud customers to review the security practices of providers, accelerating their due diligence and leading to higher quality procurement experiences.
13	Unique selling point	Industry transparency (encouraging providers to make security capabilities a market differentiator). According to the CSA website, “Cloud providers have the benefit of being recognized as a security conscious organization, and will gain exposure to information security, assurance and risk management professionals which are a key part of the cloud service procurement process. Providers will also be able to streamline their responses to customer due diligence inquiries and “one off” audits”.

		Free, publicly accessible registry.
14	Privacy/data protection elements of the scheme	Data security/access to data/data breach notifications.
15	Guarantees offered to the data subject	-
16	Steps in the certification process	<p>A provider may submit a description of its security controls to the CSA for display on the CSA STARSM Registry by doing the following:</p> <ol style="list-style-type: none"> 1. Provider must prepare a Security Disclosure, which is a written document that contains its response to the CSA Consensus Assessments Initiative Questionnaire (CAIQ) or that describes its compliance with the controls that are set forth in the CSA Cloud Controls Matrix (CCM); 2. Provider must upload the Security Disclosure and the completed STAR Application Form on the CSA STARSM website as explained in the CSA STARSM FAQs; <p>After a provider has uploaded its Security Disclosure, CSA verifies the authenticity of the submission, performs a basic check to ensure that the application is complete, and uploads the Security Disclosure on the CSA STARSM Registry.</p> <p>The CSA may refuse to post, or may delete any Security Disclosure that in its sole judgment violates its Terms.</p>
17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification cost)	CSA STAR is free for both providers to submit registry entries and for consumers to use the registry for research. According to its website, “In the future, CSA may elect to charge a fee for posting to the STAR Registry, or to limit the number of postings that a single entity may post on the CSA STAR Registry at no cost.”
19	Validity	CSA will mark entries older than one year to be deprecated, and will remove the entries completely after an additional six months.
20	Revocation mechanism	<p>CSA will mark any Security Disclosure that is older than 365 days to be deprecated, and will remove from the CSA STAR Registry obsolete Security Disclosures within six months if the Security Disclosure has not been updated.</p> <p>CSA may delete or block any or all Security Disclosures associated with Provider at any time and without notice, if CSA determines in its sole</p>

		discretion that a Provider has violated its Terms, the law, or for any other reason.
21	Recognition	-
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	-
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	<p>Providers may choose</p> <ul style="list-style-type: none"> • Either to submit a report documenting compliance with the Cloud Controls Matrix (CCM), which provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry, • Or to complete and submit The Consensus Assessments Initiative Questionnaire (CAIQ), which provides industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings.
26	Frequency and means of updates to scheme	-
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	Individuals concerned about objectively false information in the CSA STAR can contact the CSA at a designated email address.
29	Criticisms	
30	Links and references to the scheme	Savage, Marcia, “CSA cloud provider registry aims to boost cloud transparency”, <i>TechTarget</i> , 4 Aug 2011.
31	Logo	 <p>The logo for the Cloud Security Alliance (CSA) features the letters 'CSA' in a large, bold, blue font. To the right of 'CSA', the words 'cloud', 'security', and 'alliance' are stacked vertically in a smaller, orange font. A small 'SM' trademark symbol is located at the bottom right of the word 'alliance'.</p>
32	Website	https://cloudsecurityalliance.org/star/
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	Not applicable /No information provided in the Cloud Controls Matrix (CCM) .
34	Data collection for specified, explicit and legitimate purposes	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
35	Adequate, relevant and limited data collection	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
36	Data accuracy	Not with regard to personal information. With

		regard to system information, the Cloud Controls Matrix (CCM) mentions “Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.”
37	Time and purpose restricted data retention	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
38	Data is processed under the responsibility and liability of the controller	According to the Cloud Controls Matrix (CCM) , “Statutory, regulatory, and contractual requirements shall be defined for all elements of the information system. The organization's approach to meet known requirements, and adapt to new mandates shall be explicitly defined, documented, and kept up to date for each information system element in the organization. Information system elements may include data, objects, applications, infrastructure and hardware. Each element may be assigned a legislative domain and jurisdiction to facilitate proper compliance mapping.”
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
40	Consent requirement for processing of special personal data	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Listings in the STAR registry also provide access to the respective providers’ completed Consensus Assessments Initiative Questionnaire (CAIQ) , or Cloud Controls Matrix (CCM) report.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Yes (not specifically to a child). The Cloud Controls Matrix (CCM) states, “Management shall approve a formal information security policy document which shall be communicated and published to employees, contractors and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security policy shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles”.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Yes (email address to report abuse).
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure 	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .


	<ul style="list-style-type: none"> • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country • Any further information necessary to guarantee fair processing 	
46	Provision for right of access for the data subject	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
47	Provision for right to rectification	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
48	Provision for right to be forgotten and to erasure	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
49	Provision for right to data portability	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
50	Provision for data subject's right to object	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
52	Rights in relation to automated processing	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
53	Documentation requirements (Art 28)	Not applicable/No information provided in the CCM.
54	Implementing the data security requirements (Article 30)	Yes. Items 9 – 24 of the Cloud Controls Matrix (CCM) embody security requirements.
55	Notification of a personal data breach to the supervisory authority (Article 31)	The Cloud Controls Matrix (CCM) states, "Contractors, employees and third party users shall be made aware of their responsibility to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a prompt and expedient manner in compliance with statutory, regulatory and contractual requirements. Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents."
56	Communication of a personal data breach to the data subject (Article 32)	The Cloud Controls Matrix (CCM) states, "In the event a follow-up action concerning a person or organization after an information security incident requires legal action proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction".
57	Data protection impact assessment (Article 33)	The Cloud Controls Matrix (CCM) states, "Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all

		identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).”
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
59	Designation of a data protection officer (Article 35(1))	Not applicable/No information provided in the Cloud Controls Matrix (CCM) .
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)

11.4 CNIL LABEL

	General criteria for evaluation and comparison of privacy seals	CNIL label
1	Nature (privacy-oriented/general trust mark)	Privacy/data protection label
2	Country	France
3	Inception	2011
4	Issuing organisation	Commission Nationale de l'Informatique et des Libertés" (CNIL), the French Data Protection Authority.
5	Issuer type	Data Protection Authority. Independent administrative authority.
6	Target of scheme	Procedures concerning personal data processing.
7	Number of certified entities	According to its July 2013 press release, CNIL had 36 applications and issued 20 labels.
8	Renewals	Labels can be renewed 6 months before expiry (renewal is not automatic).
9	Types of entities that can be certified	Initially, companies that provide privacy training and audit procedures.
10	Type of beneficiaries	Certified entities, users or products and procedures, and the public.
11	Objective of scheme	To indicate to the public that the process or the product meets the CNIL's standards and is in conformity with the Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended) . To improve user confidence in privacy protection by certified products and services.
12	Descriptive summary of scheme	The CNIL issues a quality-label to products or procedures intended to protect individuals in respect of processing of personal data, once it has recognised them to be in conformity with its standards and with the provisions of Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended) . The CNIL maintains on its website a list of certified products and processes. The certified entity is permitted to use the CNIL label.
13	Unique selling point	Label is issued by data protection authority.
14	Privacy/data protection elements of the scheme	Applicability of provisions of Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended) .
15	Guarantees offered to the data subject	In line with the provisions of Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended) .

16	Steps in the certification process	<ol style="list-style-type: none"> 1. Download application. 2. Applicant to explain how product, procedure meets the CNIL requirements and provide description and other details such as audit repository, internal procedures. File application. 3. The CNIL analyses the admissibility of the application within 2 months after filing. 4. If application is admissible then the CNIL analyses whether the product or process complies with its requirements specified in its repository. 5. The CNIL may seek evaluation of an independent qualified person, when justified by the complexity of the product or of the procedure. The cost of such evaluation shall be borne by the applicant. 6. Exchanges between the Commission and the applicant to clarify certain points. 7. Presentation in the plenary Commission for decision on granting (or not) the label. The applicant may withdraw its application for a label at any time. 8. The decision to grant the label takes the form of a resolution which is transmitted to the applicant and published on Légifrance.
17	Coverage of international transfers	Covered in Articles 22, 30 and 31 and Chapter XII of Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended) .
18	Costs (i.e., evaluation cost, certification cost)	The evaluation is free when it is performed by the CNIL. Currently this is the only scheme implemented. However, the law provides that the president of the CNIL can seek the evaluation of an independent qualified person, when justified by the complexity of the product or of the procedure. In that case, the cost of such evaluation shall be borne by the company requesting the label.
19	Validity	Three years.
20	Revocation mechanism	A label may be revoked for non-compliance with CNIL criteria. The CNIL informs the label holder of the challenge to the label and gives it a month to respond. If the holder does not provide the CNIL with satisfactory information, a rapporteur presents the facts to the Commission which then makes a decision on revocation of the label.
21	Recognition	-
22	Accredited experts and/or evaluation bodies	None. All evaluations are currently performed by the CNIL staff.
23	Duration and scope of the certification process	The time needed for instruction may vary depending on the complexity of the product or procedure.

24	Number of certified experts and/or bodies	Comité de labellisation comprising three CNIL Commissioners.
25	Regulatory/ compliance standards	CNIL standards for labelling of products and procedures based on the Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (as amended) . Délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés (chapitre V, section 2). The requirements are outlined in the "referentiel" which is published for each procedure or product.
26	Frequency and means of updates to scheme	The CNIL may change its repository. Labels granted under old framework remain valid. However, if these are sought to be renewed they must demonstrate compliance of the product/procedure to the new standards.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	Any person (user of the product or procedure) can complain to the CNIL. The label has a dedicated email id.
29	Criticisms	On 5 January 2007, CNIL reportedly censured "certain companies marketing biometric technology in the form of fingerprint(s) recognition systems pretended to have received a CNIL label or a CNIL approval". See Winston & Strawn LLP, "Biometrics: French officials warning", <i>Briefing</i> , February 2007.
30	Links and references to the scheme	• <i>O'Donoghue, Cynthia & Daniel Kadar</i> , " Labels of conformity with the French Data Protection Act now available from the CNIL ", <i>Global Regulatory Enforcement Law Blog</i> , 9 December 2011.
31	Logo	
32	Website	http://www.cnil.fr/linstitution/labels-cnil/
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	Article 6 (1) of the Loi Informatique et Libertés .
34	Data collection for specified, explicit and legitimate purposes	Article 6 (2) of the Loi Informatique et Libertés .

35	Adequate, relevant and limited data collection	Article 6 (3) of the Loi Informatique et Libertés .
36	Data accuracy	Article 6 (4) of the Loi Informatique et Libertés .
37	Time and purpose restricted data retention	Article 6 (5) of the Loi Informatique et Libertés .
38	Data is processed under the responsibility and liability of the controller	Not specified as such.
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not specified as such.
40	Consent requirement for processing of special personal data	Article 8 (1) of the Loi Informatique et Libertés .
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Article 32 of the Loi Informatique et Libertés .
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Article 32 of the Loi Informatique et Libertés .
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Section 2 of the Loi Informatique et Libertés covers rights of individuals in respect of processing of personal data.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	-
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequate decision by the Commission • Any further information necessary to guarantee fair processing 	Article 57 of the Loi Informatique et Libertés provides: The individuals from whom the personal data are obtained or whose data are transmitted shall, before the start of the processing of these data, be informed individually of: 1° the nature of the transmitted information; 2° the purpose of the data processing; 3° the individuals or legal entities who are the recipients of the data; 4° the right of access and the rectification provided for in Articles 39 (right of access) and 40 (right of rectification); 5° the right to object provided for in the first (objection to the lifting of professional secrecy) and third (refusal of processing after death) paragraphs of Article 56 or, in the case provided for in the second paragraph of this Article, about the obligation to obtain their consent.
46	Provision for right of access for the data subject	Article 39 the Loi Informatique et Libertés .
47	Provision for right to rectification	Articles 6 (4), 40 of the Loi Informatique et Libertés - Appropriate steps shall be taken in order to delete and rectify data that are inaccurate and incomplete with regard to the purposes for which they are obtained and processed.
48	Provision for right to be forgotten and to erasure	Articles 6 (4) of the Loi Informatique et Libertés - Appropriate steps shall be taken in order to delete and rectify data that are inaccurate and


		<p>incomplete with regard to the purposes for which they are obtained and processed.</p> <p>Article 40 - Any individual providing proof of identity may ask the data controller to, as the case may be, rectify, complete, update, block or delete personal data relating to him that are inaccurate, incomplete, equivocal, expired, or whose collection, usage, disclosure or storage is prohibited.</p>
49	Provision for right to data portability	-
50	Provision for data subject's right to object	Article 38 of the <u>Loi Informatique et Libertés</u> provides that "any natural person is entitled, on legitimate grounds, to object to the processing of any data relating to him".
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Article 38 of the <u>Loi Informatique et Libertés</u> states: Any natural person is entitled, on legitimate grounds, to object to the processing of any data relating to him. He is entitled to object, at no cost to himself, to the use of the data relating to him for purposes of canvassing, in particular for commercial ends, by the controller of a current or a further data processing.
52	Rights in relation to automated processing	Articles 2, 10, 11 (2) (d), 22, 25, 31, 39 (5), 54 of the <u>Loi Informatique et Libertés</u> .
53	Documentation requirements (Art 28)	Article 22 of the <u>Loi Informatique et Libertés</u> provides the data protection officer "shall keep a list of the processing carried out, which is immediately accessible to any person applying for access".
54	Implementing the data security requirements (Article 30)	Article 34 of the <u>Loi Informatique et Libertés</u> provides that the data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties.
55	Notification of a personal data breach to the supervisory authority (Article 31)	Article 34 prime of the <u>Loi Informatique et Libertés</u> .
56	Communication of a personal data breach to the data subject (Article 32)	Article 34 prime of the <u>Loi Informatique et Libertés</u> states: Whenever said violation is likely to breach personal data security or the privacy of a subscriber or any other individual, the provider shall also notify the party affected forthwith. Notification of a breach of personal data to the affected party shall however not be required if the CNIL has found that appropriate protection measures have been implemented by the service provider to ensure that the personal data are made undecipherable to any unauthorized individuals and have been applied to the data affected by said breach. Failing this, the CNIL may serve the service provider with a formal notice to inform the affected parties as well, after

		investigating the severity of the breach.
57	Data protection impact assessment (Article 33)	Not specified.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Chapter IV of the Loi Informatique et Libertés prescribes formalities prior to commencing data processing. Article 22 states: I. - Automatic processing of personal data must be notified to the CNIL except when the processing falls under the provisions of Articles 25 (political, philosophical, medical, sexual life data; genetic data; offences; exclusion from a right; combination; use of NIR, i.e. social security number), 26 (State security and criminal offences processing) and 27 (public processing of NIR– State biometrics – census – online services) that are indicated in paragraph 2 of Article 36 (conservation of archives).
59	Designation of a data protection officer (Article 35(1))	Article 22 (III) of the Loi Informatique et Libertés .
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	Chapter VI of the Loi Informatique et Libertés covers supervision of the implementation of data processing.

11.5 COMODO SECURE

	General criteria for evaluation and comparison of privacy seals	Comodo Secure
1	Nature (privacy-oriented/general trust mark)	Comodo has two trust logos – Comodo Corner of Trust and Comodo Standard TrustLogo. There are three types of TrustLogos – card payment seal, official partners seal and Site Credentials Premium Seal. General trust marks.
2	Country	UK
3	Inception	2002.
4	Issuing organisation	Comodo CA Limited
5	Issuer type	Private computer and internet security company.
6	Target of scheme	Websites.
7	Number of certified entities	Data not found.
8	Renewals	Data not found.
9	Types of entities that can be certified	Website businesses.
10	Type of beneficiaries	Businesses and consumers
11	Objective of scheme	To enable merchants to quickly build trust with online visitors.
12	Descriptive summary of scheme	According to the website : The TrustLogo is deployed using Comodo's innovative 'Point to Verify™ technology. Website users can request a real-time identity verification of the website displaying the TrustLogo by simply hovering their mouse over the logo. The identity of the website is then verified using Comodo's Identity Assurance infrastructure in real-time, and a summary of the site's credentials are displayed to the visitor. Further essential site details are available by clicking on the TrustLogo itself.
13	Unique selling point	Use of point to verify technology.
14	Privacy/data protection elements of the scheme	Applicable rules on the protection of personal data deemed by law or the Comodo privacy policy .
15	Guarantees offered to the data subject	<ul style="list-style-type: none"> • That all personnel in trusted positions will handle all information in strict confidence. • Personnel of registration authorities must comply with the requirements of the English law on the protection of personal data.
16	Steps in the certification process	Every TrustLogo application is reviewed by Comodo's validation personnel. Comodo validates applications and issues TrustLogos within two working days from application. Once the application for a TrustLogo is approved, the applicant can incorporate the TrustLogo to its website by adding simple JavaScript to the website's HTML.

17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification cost)	The charges for the subscription Service are defined on the website and specified during the online registration.
19	Validity	The TrustLogo validity commences from the date of issue and continues for the period specified by the subscriber in the enrolment form during online registration and paid for by the subscriber in accordance with the charges set out or until revocation of the TrustLogo by Comodo in accordance with the terms of its Agreement, whichever is earlier.
20	Revocation mechanism	Comodo may revoke a TrustLogo upon receipt of a valid request to revoke a certificate from a person authorized to request revocation using the revocation methods detailed in the Comodo Certification Practice Statement .
21	Recognition	Comodo is a recognised online trust and security company. However, in a survey on consumer recognition of trust logos and its effect on online purchasing , Comodo scored the worst out of all the seal providers despite having three different logos present in the test.
22	Accredited experts and/or evaluation bodies	TrustLogos are powered by the IdAuthority® - a large, real-time website identity assurance infrastructure.
23	Duration and scope of the certification process	Each TrustLogo application is reviewed by Comodo's validation personnel who ensure that the application is validated and the TrustLogo is issued within two working days from application.
24	Number of certified experts and/or bodies	Comodo is a Certification Authority with the contractual responsibility of issuing digital certificates (SSL and TrustLogo products) to subscribers (end entity web sites).
25	Regulatory/ compliance standards	TrustLogos are issued in accordance with the Comodo Certification Practice Statement - a policy document outlining the rules and practices employed in the application, issuance and management of Comodo's InstantSSL Certificate solutions and TrustLogo website identity assurance solutions. Subscribers must also comply with the TrustLogo Subscriber Agreement .
26	Frequency and means of updates to scheme	As required. See http://www.comodo.com/about/comodo-agreements.php
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	A person relying on Comodo services is protected under the Relying Party Agreement and has the right to report alleged breaches of service agreement by subscribers. Comodo will investigate the complaint and take action

		<p>accordingly.</p> <p>Complainants can email Comodo with the following information: full name, address, contact details, business name, address and business details if applicable; nature & background of complaint; URL and business details of subscriber (e.g. site for which you are making a complaint) and dates/times of alleged illegal behaviour.</p>
29	Criticisms	Though the Comodo trust mark has been said to look trustworthy, it does not have a secure link.
30	Links and references to the scheme	TNO/Intrasoft, <i>EU online Trust marks: Building Digital Confidence in Europe</i> , A study prepared for the European Commission DG Communications Networks, Content & Technology, Final report, 2012.
31	Logo	
32	Website	<p>http://www.comodo.com/e-commerce/site-seals/corner-trust.php</p> <p>http://www.trustlogo.com/</p>
General data protection regulation requirements under Ch II and III		
33	Fair, lawful, transparent processing of personal data	According to the TrustLogo Subscriber Agreement , the subscriber warrants, represents and undertakes that: all subscriber data is, and any other documents or information provided by the subscriber are, and will remain accurate and will not include any information or material (or any part thereof), the accessing or use of which would be unlawful.
34	Data collection for specified, explicit and legitimate purposes	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
35	Adequate, relevant and limited data collection	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
36	Data accuracy	According to the TrustLogo Subscriber Agreement , the Subscriber warrants, represents and undertakes that: all subscriber data is, and any other documents or information provided by


		the subscriber are, and will remain accurate and will not include any information or material (or any part thereof), the accessing or use of which would be unlawful, contrary to public interest or otherwise likely to damage the business or reputation of Comodo in any way.
37	Time and purpose restricted data retention	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
38	Data is processed under the responsibility and liability of the controller	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
40	Consent requirement for processing of special personal data	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	The subscriber is to provide the following subscriber data: company name (ssid), street address, post box, city (ssid), county/state (ssid), postal/zip code, domain name (ssid), subscriber's corporate logos, account user name, account password, administrator contact details. The subscriber shall optionally provide: either or both separate billing contact and organisational contact details, business description, URL of subscriber privacy statement, URL of subscriber terms & conditions, URL of shipping details, URL of returns policy, customer contact telephone number, customer contact fax number, customer complaints email contact, customer feedback email, customer support email, webmaster contact email and up to three self-defined email addresses, and an acknowledgement of Subscriber's consent to the terms of this Agreement. Items marked 'ssid' will either be embedded into the subscriber's TrustLogo and all other data referenced shall be made available to the relying party via the

		TrustLogo Service.
46	Provision for right of access for the data subject	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
47	Provision for right to rectification	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
48	Provision for right to be forgotten and to erasure	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
49	Provision for right to data portability	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
50	Provision for data subject's right to object	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
52	Rights in relation to automated processing	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
53	Documentation requirements (Art 28)	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
54	Implementing the data security requirements (Article 30)	TrustLogo Subscriber Agreement : The subscriber shall take all reasonable measures to ensure the security and proper use of all personal identification numbers, private keys and passwords used in connection with the subscription service.
55	Notification of a personal data breach to the supervisory authority (Article 31)	TrustLogo Subscriber Agreement : the subscriber shall also immediately inform Comodo if there is any reason to believe that a personal identification number, private key or password has or is likely to become known to someone not authorised to use it, or is being, or is likely to be used in an unauthorised way.
56	Communication of a personal data breach to the data subject (Article 32)	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
57	Data protection impact assessment (Article 33)	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
59	Designation of a data protection officer (Article 35(1))	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	Not specified in the Comodo Certification Practice Statement or TrustLogo Subscriber Agreement .

11.6 CONFIANZA ONLINE

	General criteria for evaluation and comparison of privacy seals	Confianza Online
1	Nature (privacy-oriented/general trust mark)	General trust mark
2	Country	Spain
3	Inception	1998 (Code of Data Protection on the Internet issued by Adigital), 1999 (Autocontrol's Ethical Code for Internet Advertising).
4	Issuing organisation	Confianza Online
5	Issuer type	Non-profit, private sector association
6	Target of scheme	Different sectors of information society (to date: commercial communications, commerce/ economic transactions with consumers and security in transactions, minor protection; accessibility/usability; privacy and data protection).
7	Number of certified entities	2,556
8	Renewals	-
9	Types of entities that can be certified	Internet/e-commerce businesses (Any physical person or public or private entity with an institutional, corporate, or commercial website that agrees to comply with Confianza's Ethical Code may apply for certification).
10	Type of beneficiaries	Internet/e-commerce users, consumers
11	Objective of scheme	<ul style="list-style-type: none"> To increase consumer's confidence in e-commerce and interactive advertising. To provide public and private entities with a perfect tool for demonstrating to consumers the ethical commitment they have made to society in the realm of e-commerce and interactive advertising. To provide online consumers and businesses with a quick, inexpensive, and effective extrajudicial mechanism for solving disputes beyond the current fragmentary legislation of global regulations.
12	Descriptive summary of scheme	According to its website , "Confianza Online guarantees that the company which displays its logo has made a serious commitment to self-regulation. Adhered members voluntarily commit to respect Confianza Online's Ethical Code in all their activities and yield to any complaints made against them for infractions of the rules of the Ethical Code, through the extrajudicial dispute resolution system established for them. Adhered members have the right to display the Confianza Online trust mark on those websites which they own and included in their application thus informing users and potential clients that they form part of

		the association”.
13	Unique selling point	(Relevant to Spain): <ul style="list-style-type: none"> • More than 10 associations representing the areas of new digital media, e-commerce and advertising in Spain participated in its original drafting, making it a representative self-regulation code of the sector. • By including Confianza Online’s trust mark on their web pages, certified entities are also able to make visible their commitment to the ethical rules which the Code entails.
14	Privacy/data protection elements of the scheme	Title IV of the Ethical Code .
15	Guarantees offered to the data subject	-
16	Steps in the certification process	An applicant has to fill out the online application form, which lists the fees for this tax year, and send it to Confianza Online by post. The dues are paid and the process of verifying the website gets under way. Confianza Online’s Technical Secretariat analyses the legal aspects of the website including information about the business, information prior to the contracting of products or services, information about data protection, browsing notices for minor protection, etc. Once the business has made any changes requested, it can start using the trust mark.
17	Coverage of international transfers	Yes, see Article 28 of the Ethical Code .
18	Costs (i.e., evaluation cost, certification cost)	Calculated according to volume of sales, as follows: A) companies billing less than €1,000,000: €295 + VAT B) companies billing between €1,000,001 and €5,000,000: €550 + VAT C) companies billing between €5,000,001 and €10,000,000: €1250 + VAT D) companies billing between €10,000,001 and €25,000,000: €2,400 + VAT E) companies billing more than €25,000,001: €3,500 + VAT There are also fees for claim settlement/administration.
19	Validity	-
20	Revocation mechanism	-
21	Recognition	-
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	The acquisition of Confianza Online’s trust mark is tied directly to the verification of the website requesting it. The time it takes to accept


		the website depends on its compliance with the rules of Confianza Online's Ethical Code . If Confianza Online detects a discrepancy, it will be communicated to the company so that it may make the necessary changes.
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	The Ethical Code entered into force in 2003 and was amended in 2005, 2009 and 2011. The Ethical Code consists of a set of ethical standards divided into 5 major areas: <ul style="list-style-type: none"> - Commercial communications - E-commerce with consumers - Protection of personal data - Protection of minors and adolescents - Accessibility and usability
26	Frequency and means of updates to scheme	-
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	Consumers may submit a complaint either by post or through an online form. Once received, the Confianza Online Technical Secretariat contacts the interested parties. Consumers may also file a complaint against businesses not participating in the Confianza Online scheme; Confianza Online attempts to mediate.
29	Criticisms	There have been consumer complaints with regard to efficiency of the process in consumer blogs. (for instance, http://www.ciao.es/Opiniones/confianzaonline.org_404068)
30	Links and references to the scheme	Suquet, Josep, et al, "Online Dispute Resolution in 2010: A Cyberspace Odyssey?", <i>Proceedings of the 6th International Workshop on Online Dispute Resolution</i> , Liverpool, United Kingdom, 2010.
31	Logo	
32	Website	http://www.confianzaonline.es
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent	Yes, see Article 23 of the Ethical Code .

	processing of personal data	
34	Data collection for specified, explicit and legitimate purposes	Yes, see Articles 23 and 25 of the Ethical Code .
35	Adequate, relevant and limited data collection	Yes, see Article 23 of the Ethical Code .
36	Data accuracy	Yes, see Article 23 of the Ethical Code .
37	Time and purpose restricted data retention	Yes, see Article 23 of the Ethical Code .
38	Data is processed under the responsibility and liability of the controller	-
39	Provision for parental consent based processing of personal data of a child below the age of 13	Yes, see Title V of the Ethical Code .
40	Consent requirement for processing of special personal data	-
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Yes, see Article 30 of the Ethical Code .
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Yes, see Article 30 and Title V of the Ethical Code .
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Yes, see Article 30 of the Ethical Code .
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	-
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data be stored • Existence of the right to request access and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients personal data • Transfer to a third country or international organisation and on the level of protection afforded by that country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	Yes, see Articles 24 and 30 of the Ethical Code (except international transfers)

46	Provision for right of access for the data subject	Yes, see Article 30 of the Ethical Code .
47	Provision for right to rectification	Yes, see Article 30 of the Ethical Code .
48	Provision for right to be forgotten and to erasure	-
49	Provision for right to data portability	-
50	Provision for data subject's right to object	Yes, see Article 30 of the Ethical Code .
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Yes, see Articles 26 and 27 of the Ethical Code .
52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	-
54	Implementing the data security requirements (Article 30)	Yes, see Article 33 of the Ethical Code .
55	Notification of a personal data breach to the supervisory authority (Article 31)	-
56	Communication of a personal data breach to the data subject (Article 32)	-
57	Data protection impact assessment (Article 33)	-
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	-
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	-

11.7 DANISH E-MARK

	General criteria for evaluation and comparison of privacy seals	Danish e-mark (e-mærket)
1	Nature (privacy-oriented/general trust mark)	General trust mark (official Danish accreditation for safe and ethically responsible conduct and trade on the Internet).
2	Country	Denmark
3	Inception	-
4	Issuing organisation	The e-commerce Foundation (e-handelsfonden) established by the Danish Consumer Council, the Danish Chamber of Commerce, the Danish Bankers' Association, the Confederation of Danish Industries, the Union of Commercial and Clerical Employees, ITEK, Danish IT Society, ITK, The Danish IT Industry Association and the Danish e-business Association).
5	Issuer type	Non-profit trust
6	Target of scheme	Internet sellers/consumers
7	Number of certified entities	1,475
8	Renewals	-
9	Types of entities that can be certified	Online businesses
10	Type of beneficiaries	Consumers
11	Objective of scheme	To help increase consumer confidence online regarding payment, treatment of personal information, use of e-mail addresses, and with regards to guarantees and agreements.
12	Descriptive summary of scheme	-
13	Unique selling point	-
14	Privacy/data protection elements of the scheme	-
15	Guarantees offered to the data subject	According to one of the subscribers to the scheme, the scheme guarantees include no spam, easy access to information concerning the use of personal data and that consumers/users will not be sent newsletters or electronic advertising without their expressed consent.
16	Steps in the certification process	Application is made by submitting an electronic form. Upon application, an initial review of compliance with the code of conduct is carried out. The organisation carries out both an annual check and random checks.
17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification	According to a study by conducted on


	cost)	behalf of the European Consumer Centre, Denmark , “The costs depend on the number of employees in the business, and there is an initial application fee and an annual fee. The application fee ranges from €280 to €1000, and the annual fee ranges between €450 and €1750. The application fee is paid per website, but discounts are available for businesses with multiple websites”.
19	Validity	-
20	Revocation mechanism	In case of non-compliance, the business is given 30 days to comply. If the business does not comply, the business is not permitted to display the mark.
21	Recognition	-
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	-
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	-
26	Frequency and means of updates to scheme	-
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness)	-
28	Complaints mechanism	-
29	Criticisms	Not found.
30	Links and references to the scheme	Trzaskowski, Jan, E-Commerce Trust marks in Europe , 2006.
31	Logo	
32	Website	https://www.emaerket.dk
	General data protection regulation requirements under Ch II and III	Note: GDPR related analysis was not possible due to lack of information and non-availability of information in any language other than Danish.
33	Fair, lawful, transparent processing of personal data	-
34	Data collection for specified, explicit and legitimate purposes	-
35	Adequate, relevant and limited data collection	-
36	Data accuracy	-
37	Time and purpose restricted data retention	-
38	Data is processed under the responsibility	-

	and liability of the controller	
39	Provision for parental consent based processing of personal data of a child below the age of 13	-
40	Consent requirement for processing of special personal data	-
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	-
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	-
43	Existence of procedures and mechanisms for exercising the rights of the data subject	-
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	-
45	Provision of information to data subject: <ul style="list-style-type: none"> • Identity and the contact details of the controller purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	-
46	Provision for right of access for the data subject	-
47	Provision for right to rectification	-
48	Provision for right to be forgotten and to erasure	-
49	Provision for right to data portability	-
50	Provision for data subject's right to object	-
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	-
52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	-
54	Implementing the data security requirements (Article 30)	-
55	Notification of a personal data breach to the supervisory authority (Article 31)	-
56	Communication of a personal data breach to the data subject (Article 32)	-

57	Data protection impact assessment (Article 33)	
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	-
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	-

11.8 EPRIVACY SEAL

	General criteria for evaluation and comparison of privacy seals	ePrivacyseal
1	Nature (privacy-oriented/general trust mark)	Privacy-oriented trust mark
2	Country	Germany
3	Inception	-
4	Issuing organisation	ePrivacyseal GmbH / ePrivacyconsult GmbH
5	Issuer type	Private sector (consulting) company
6	Target of scheme	Companies offering web and mobile pages and digital communication services.
7	Number of certified entities	10 (See List)
8	Renewals	-
9	Types of entities that can be certified	Private companies
10	Type of beneficiaries	Digital consumers
11	Objective of scheme	To build confidence with users and customers and to convey privacy commitments.
12	Descriptive summary of scheme	According to its website , “The ePrivacyseal is a provider of online data protection solutions for global certification standards and awards the Privacy Seal” for exemplary respect of digital privacy. The certification is stated to be based on the German and EU data protection law and including the IAB Europe Agreements OBA, (however there is a potential contradiction between German and EU data protection law and IAB terms Article 5(3) and it is not clear how ePrivacyseal resolves this). The ePrivacyseal is awarded for good ratings of technical and legal aspects. The criteria are the same for all companies.
13	Unique selling point	The seal sets high data protection standards in line with EU legal requirements as well as national legislation in relation to transparency, choice and accountability in relation to the collection and use of personal data.
14	Privacy/data protection elements of the scheme	German and EU data protection law (including the IAB Europe Agreements OBA).
15	Guarantees offered to the data subject	-
16	Steps in the certification process	According to ePrivacyseal’s website , the certification process involves the following: <p>1. Legal aspects</p> <p>Actual status analysis of conformity to the requirements of German Data Protection Act (BDSG), Telemedia Act (Telemediengesetz) and EU legislation. Consulting on concepts of data protection, legal frameworks and technologies as well as online marketing. <i>Optional verification of conformity with national legislation in Switzerland, Russia, USA and elsewhere.</i></p>

		<p>2. Technical aspects Data protection verification and scanning for possible non-compliance with the requirements of data protection. <i>Optional verification of downstreamed processes.</i></p> <p>3. ePrivacy data protection seal Certification in line with the German Data Protection Act (BDSG) and the award of the ePrivacy quality label for web and mobile pages and digital communication services. <i>Optional up-to-date declaration of data protection for web pages and other digital communication services, external data protection officers on demand BDSG Certification (German Data Protection Act)</i></p>
17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification cost)	-
19	Validity	-
20	Revocation mechanism	-
21	Recognition	-
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	-
24	Number of certified experts and/or bodies	Two certified experts.
25	Regulatory/ compliance standards	EU/German law /IAB OBA Framework The Criteria documents are available on the website .
26	Frequency and means of updates to scheme	-
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	ePrivacyseal offers preliminary certification services for the IAB Europe OBA Framework. Companies which successfully pass the certification are awarded the trusted seal.
28	Complaints mechanism	-
29	Criticisms	-
30	Links and references to the scheme	-
31	Logo	
32	Website	http://www.eprivacyconsult.com
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	Yes, Art. I.2 of the Criteria Catalogue .
34	Data collection for specified, explicit and legitimate purposes	Yes, Art. I.3,4 of the Criteria Catalogue .

35	Adequate, relevant and limited data collection	Yes, Art. I.1 of the Criteria Catalogue .
36	Data accuracy	-
37	Time and purpose restricted data retention	Yes, Art. I.1,2 of the Criteria Catalogue .
38	Data is processed under the responsibility and liability of the controller	Yes, Chapter IV of the Criteria Catalogue .
39	Provision for parental consent based processing of personal data of a child below the age of 13	-
40	Consent requirement for processing of special personal data	Yes, Art. II.4 of the Criteria Catalogue .
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Yes, Art. I.2(b) of the Criteria Catalogue .
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	-
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Yes, Chapter III of the Criteria Catalogue .
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Yes, Art. III.2,3,4 of the Criteria Catalogue .
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	Yes, Art. I.2, III.1 of the Criteria Catalogue (except international data transfers).
46	Provision for right of access for the data subject	Yes, Art. III.1 of the Criteria Catalogue .
47	Provision for right to rectification	Yes, Art. III.2 of the Criteria Catalogue .
48	Provision for right to be forgotten and to erasure	-
49	Provision for right to data portability	-
50	Provision for data subject's right to object	Yes, Art. III.4 of the Criteria Catalogue .
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Yes, Chapter V of the Criteria Catalogue (OBA Framework).
52	Rights in relation to automated processing	Yes, Art. II.5 of the Criteria Catalogue .
53	Documentation requirements (Art 28)	Yes, Chapter IV of the Criteria Catalogue .
54	Implementing the data security requirements (Article 30)	Yes, Chapter IV (particularly, IV.4) of the Criteria Catalogue .


55	Notification of a personal data breach to the supervisory authority (Article 31)	-
56	Communication of a personal data breach to the data subject (Article 32)	-
57	Data protection impact assessment (Article 33)	-
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	Yes, Art. IV.1 of the Criteria Catalogue .
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	-

11.9 ESRB PRIVACY ONLINE CERTIFICATION

	General criteria for evaluation and comparison of privacy seals	ESRB Privacy Online Certification
1	Nature (privacy-oriented/general trust mark)	Privacy certification seals of three types: <ul style="list-style-type: none"> • ESRB Kids Privacy Certified seal • ESRB Privacy Certified seal for websites and mobile apps • ESRB EU Privacy Certified seal
2	Country	USA
3	Inception	1999
4	Issuing organisation	The Entertainment Software Rating Board (ESRB)
5	Issuer type	Non-profit, self-regulatory body.
6	Target of scheme	<ul style="list-style-type: none"> • The ESRB Kids Privacy Certified seal applies to websites or mobile apps directed to children under 13 (12 years and younger) or to any company with actual knowledge that it collects personal information from children under 13. • The ESRB Privacy Certified seal is for websites and mobile apps directed to users 13 and over • The ESRB EU Privacy Certified seal is targeted at companies doing business with EU based consumers.
7	Number of certified entities	According to the website , the program supports over 2,000 websites and apps. A full list of websites is available at: http://www.esrb.org/privacy/sites.jsp
8	Renewals	-
9	Types of entities that can be certified	<ul style="list-style-type: none"> • Companies with websites, mobile apps • A company with actual knowledge that it collects personal information from children under 13 • Companies doing business with EU based consumers
10	Type of beneficiaries	<ul style="list-style-type: none"> • The ESRB Kids Privacy Certified seal - beneficiaries are children under 13, parents. • The ESRB Privacy Certified seal is for websites and mobile apps - beneficiaries are website, mobile app users, consumers. • The ESRB EU Privacy Certified seal - beneficiaries are EU-based consumers.
11	Objective of scheme	According to its website , ESRB's Privacy Online Program aims to help "interactive software companies conduct business

		responsibly while assuring consumers, especially parents, that their personal data is collected and managed appropriately through the display of our Privacy Certified seal” and “mitigate their risk and achieve business objectives by providing guidance in developing the most effective privacy practices consistent with applicable law”.
12	Descriptive summary of scheme	<ul style="list-style-type: none"> • The ESRB Kids Privacy Certified seal applies if any part of a member's website or mobile app is directed to children under 13 (12 years and younger) or if a company has actual knowledge that it collects personal information from children under 13. U.S. federal law requires such products to comply with the requirements of the Children's Online Privacy Protection Rule (16 C.F.R. Part 312). • The ESRB Privacy Certified seal is for websites and mobile apps directed to users 13 and over. • The ESRB EU Privacy Certified seal assures EU-based consumers that a member website is in compliance with the EU Data Protection Directive and cookie law when/if collecting personal information.
13	Unique selling point	<ul style="list-style-type: none"> • Takes into account laws, regulations of US, Canada, Europe Union (EU), the Asia-Pacific region and South America. • Companies collecting and using highly sensitive personal information are held to a higher standard of verification (verification may necessitate that the participating company hire an outside auditor to review the compliance record). • Children's seal program
14	Privacy/data protection elements of the scheme	<ul style="list-style-type: none"> • Notice/disclosure • Choice • Limiting collection and retention of personal information • Data integrity/security • Data access • Enforcement/accountability • Children's Program Requirements
15	Guarantees offered to the data subject	<ul style="list-style-type: none"> • Notice/disclosure • Choice • Limiting collection and retention of personal information • Data integrity/security • Data access • Enforcement/accountability

		<ul style="list-style-type: none"> Children's guarantees
16	Steps in the certification process	<ol style="list-style-type: none"> Complete a Privacy Self-Assessment Questionnaire. Responses to the questionnaire help ESRB assess a company's existing privacy practices. Submit to a review of information collection practices. The ESRB reviews the company's website, identifies required changes and recommends areas of improvement before certifying the website. After completing a thorough assessment of a member's website or mobile app, ESRB identifies what the privacy policy should include and remains available for ongoing consultation throughout the life of the product.
17	Coverage of international transfers	Not specified.
18	Costs (i.e., evaluation cost, certification cost)	One-time annual fee plus annual assessment evaluation fee. Exact rates not found on website.
19	Validity	Not clear.
20	Revocation mechanism	Failure to take the corrective actions can result in a number of penalties including the imposition of fines, removal of the ESRB Privacy Online Certification Seal, and referral to the US Federal Trade Commission.
21	Recognition	According to ESRB's website, it is "among the first privacy seal programs sanctioned by the Federal Trade Commission (FTC) as an authorized "Safe Harbor" under the Children's Online Privacy Protection Act (COPPA) ".
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	Not clear.
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	<p>The ESRB Principles and Guidelines.</p> <p>The ESRB Kids Privacy Certified seal certifies compliance with requirements of the Children's Online Privacy Protection Rule (16 C.F.R. Part 312). The ESRB Privacy Certified seal certifies compliance under COPPA in addition to compliance with US (federal and state) and foreign laws and best practices such as CAN-SPAM, PIPEDA (Canada), the EU cookie law, regulations pertaining to data breach preparedness and data storage practices, reconciliation of privacy policies with end user</p>

		<p>licence agreements or terms of service, implementation of sweepstakes, contests, e-mail campaigns and newsletters, deployment of COPPA-compliant age gates, enhanced privacy disclosures for mobile, and others.</p> <p>The ESRB EU Privacy Certified seal assures EU-based consumers that a member website complies with the EU Data Protection Directive (95/46/EC) and cookie law when collecting personal information.</p>
26	Frequency and means of updates to scheme	Not clear.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	<ul style="list-style-type: none"> Monitoring through the Sentinel Program (oversight and enforcement wing of the ESRB Privacy Online programme). Quarterly reviews of participating companies information practices.
28	Complaints mechanism	The ESRB helps member companies develop an internal dispute resolution programs and acts as mediator if required. A Consumer Online Hotline is available to consumers whose privacy concerns are not satisfactorily resolved by member companies.
29	Criticisms	<ul style="list-style-type: none"> The ESRB cannot guarantee website will not indulge in privacy invasive practices.
30	Links and references to the scheme	<ul style="list-style-type: none"> Liu, Chang & Kirk P. Arnett, “An Examination of Privacy Policies in Fortune 500 Web Sites”, <i>American Journal of Business</i>, Vol. 17 Iss. 1, 2002, pp. 13- 22. Cook, David & Wenhong Luo, “The role of third-party seals in building trust online”, <i>E-Service Journal</i> Vol. 2, No. 3, 2003, pp. 71- 84.
31	Logo	
32	Website	http://www.esrb.org/
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of	Yes. The ESRB Principles and Guidelines

	personal data	provide that “participating companies must limit the collection and retention of personal information to that which is needed for valid business reasons and any such information must be obtained by lawful and fair means”.
34	Data collection for specified, explicit and legitimate purposes	The ESRB Principles and Guidelines require that participating companies must limit the collection and retention of personal information to that which is needed for valid business reasons.
35	Adequate, relevant and limited data collection	The ESRB Principles and Guidelines clarify: Even if a participating company has a valid business reason to collect personal information from a consumer, it must only collect that personal information which is needed for such valid business reason. Participating companies must periodically re-evaluate whether a valid business reason continues to exist for collection or retention of certain personal information, and if the valid business reason ceases to exist or ceases to require the collection or retention of certain personal information, participating companies must limit their collection and retention practices accordingly.
36	Data accuracy	The ESRB Principles and Guidelines suggest “Ensuring that personal information is reliable means that it is accurate, complete, and timely.”
37	Time and purpose restricted data retention	The ESRB Principles and Guidelines require participating companies to “periodically re-evaluate whether a valid business reason continues to exist for collection or retention of certain personal information, and if the valid business reason ceases to exist or ceases to require the collection or retention of certain personal information, participating companies must limit their collection and retention practices accordingly”.
38	Data is processed under the responsibility and liability of the controller	Not specified as such.
39	Provision for parental consent based processing of personal data of a child below the age of 13	The ESRB Children’s Privacy Program requirements specify: Participating companies must make reasonable efforts, taking into account available technology, to ensure that a parent receives notice of the participating company's information practices, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented. With certain exceptions, participating companies must provide notice to parents and obtain prior verifiable parental consent before collecting any personal information from a child (12 years and

		under).
40	Consent requirement for processing of sensitive personal data	<p>The ESRB Principles and Guidelines recognise the “<i>sensitivity of the data</i>”. According to the ESRB, “sensitive personal information requires a greater level of consumer choice than mere demographic information”.</p> <p>The ESRB Principles and Guidelines call for participating companies to obtain prior verifiable parental consent before collecting, using, or disclosing a child's personal information. Participating companies must also obtain prior verifiable parental consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.</p>
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	<p>The ESRB Principle on Notice/Disclosure requires each participating company to implement and publish a Privacy Statement that informs consumers about its information practices. Further, it clarifies:</p> <p>Participating companies are required to provide a prominently displayed link to their Privacy Statement in the form of the ESRB Privacy Online Certification Seal on the first page of their website and at any point on their website where personal information is requested. Privacy Statements must be complete, clearly and understandably written, and must contain no unrelated, confusing, or contradictory information.</p>
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	<p>The ESRB Principles and Guidelines call for privacy statements to be “complete, clearly and understandably written, and must contain no unrelated, confusing, or contradictory information”. The statements must specify: what information is collected and by what means; who is collecting the information; how the personal information is used; whether personal information is shared, rented or sold to third parties; a statement of the organisation's commitment to data security; what choices consumers are offered to customise the collection and use of their personal information; what opportunities are offered for consumers to access their personal information; what the organisation's information practices are with regard to children; the steps the organisation takes to ensure data quality; the consequences, if any, of an individual's refusal to provide information; and how consumers can ask questions or file complaints.</p>

43	Existence of procedures and mechanisms for exercising the rights of the data subject	<p>The ESRB Principles and Guidelines state: Consumers must be notified of their right to choose how their personal information is handled and provided with simple, easily understood and readily available mechanisms to exercise such choice over the collection and use of their personal information.</p> <p>Consumers must have the opportunity for reasonable, appropriate access to personal information about them that a participating company holds, and must be able to correct, amend, or request the removal of that information when necessary.</p> <p>Participating companies must implement effective and affordable mechanisms that ensure compliance with their information privacy policies and provide appropriate means of recourse for consumers.</p>
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not specified as such.
45	<p>Provision of information to data subject:</p> <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	<p>According to the ESRB Principles and Guidelines, privacy statements of participating companies must (inter alia) state: what information is collected and by what means; who is collecting the information; how the personal information is used; whether personal information is shared, rented or sold to third parties; a statement of the organisation's commitment to data security; what choices consumers are offered to customize the collection and use of their personal information; what opportunities are offered for consumers to access their personal information; what the organisation's information practices are with regard to children; what steps the organisation takes to ensure data quality; the consequences, if any, of an individual's refusal to provide information; and how consumers can ask questions or file complaints.</p> <p>Right to lodge a complaint to the supervisory authority - If a participating company fails to take appropriate actions in response to a valid complaint or an ESRB Privacy Online mandate, or engages in a pattern of violating ESRB Privacy Online requirement's, ESRB may invoke the remedies and refer such company to the Federal Trade Commission for engaging in unfair and deceptive trade practices.</p>







		Transfer to third countries – not specified.
46	Provision for right of access for the data subject	<p>The ESRB Principles and Guidelines have a specific provision related to data access: Consumers must have the opportunity for reasonable, appropriate access to personal information about them that a participating company holds, and must be able to correct, amend, or request the removal of that information when necessary.</p> <p>Privacy statements must specify the opportunities available to consumers to access their personal information so they can review, correct or remove it.</p>
47	Provision for right to rectification	<p>The ESRB Principles and Guidelines have a specific provision related to data access: Consumers must have the opportunity for reasonable, appropriate access to personal information about them that a participating company holds, and must be able to correct, amend, or request the removal of that information when necessary.</p> <p>Privacy statements must specify the opportunities available to consumers to access their personal information so they can review, correct it.</p>
48	Provision for right to be forgotten and to erasure	Not specified.
49	Provision for right to data portability	Not specified.
50	Provision for data subject's right to object	No right specified as such. Only one mention of "consumer objections" in relation to inaccurate or incomplete personal information.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not specified.
52	Rights in relation to automated processing	Not specified.
53	Documentation requirements (Art 28)	
54	Implementing the data security requirements (Article 30)	The Data Integrity/Security Principle of the ESRB Principles and Guidelines states: Participating companies creating, maintaining, using or disseminating records of personal information must take reasonable measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse, or alteration.
55	Notification of a personal data breach to the	Not specified.

	supervisory authority (Article 31)	
56	Communication of a personal data breach to the data subject (Article 32)	Not specified.
57	Data protection impact assessment (Article 33)	Not specified.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not specified.
59	Designation of a data protection officer (Article 35(1))	Not specified as such. However, the ESRB Principles and Guidelines specify: “Participating companies must assign specific personnel the responsibility for monitoring compliance with privacy practices” and “a participating company must appoint identifiable, accessible, and responsive personnel to whom consumers can initially bring a grievance”.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	<p>Prior to certification, and at annual intervals thereafter, participating companies have to submit to an ESRB Privacy Online Onsite Audit conducted by ESRB staff attorneys trained in privacy law.</p> <p>The Sentinel Program oversees and enforces the ESRB Privacy Online program, and ensures compliance. The Sentinel Program is a mandatory mechanism that provides effective enforcement in three distinct ways: Sentinel Monitoring and Verification (which includes quarterly reviews of information practices), Sentinel Spot Checks (randomly scheduled, unannounced audits of their privacy practices), and Consumer Online-Hotline.</p>

11.10 EURO-LABEL

	General criteria for evaluation and comparison of privacy seals	Euro-Label
1	Nature (privacy-oriented/general trust mark)	General trust mark
2	Country	Germany/EU
3	Inception	August 2002.
4	Issuing organisation	Respective Member State organisations (Euro-Label is the European co-operation of national suppliers of Internet trust marks): Germany, Austria, Poland, Italy, France, Spain. However, the Euro-Label website features the German association (EHI Retail Institute GmbH) as rights holder and contact organisation.
5	Issuer type	Non-profit, private sector association
6	Target of scheme	Internet traders / internet consumers
7	Number of certified entities	906
8	Renewals	Traders are “retested regularly” – no further information provided.
9	Types of entities that can be certified	Internet traders
10	Type of beneficiaries	Internet consumers
11	Objective of scheme	To guarantee online traders’ trustworthiness in accordance with a European Code of Conduct for online commercial transactions. (To increase trust and security and European e-commerce)
12	Descriptive summary of scheme	Euro-Label is a European co-operative enterprise of national suppliers of Internet trust marks. Each Member State organisation (Germany, Austria, Poland, Italy, Spain and France) is responsible for issuing its own trust mark according to relevant regulations. Euro-Label publishes a ‘European Code of Conduct’ that serves as a collective minimum standard. Each issuer uses its own list of criteria that surpasses the minimum requirements of the collective Code of Conduct and meets specific national features.
13	Unique selling point	<ul style="list-style-type: none"> • A European co-operation initiative • Free third party complaints management. • Cross-border complaints are handled in English or local language. (Haslinger, 2009)

14	Privacy/data protection elements of the scheme	<ul style="list-style-type: none"> • Basic data protection principles and data subject rights in Article 2 of the European Code of Conduct. • Protection for children personal data.
15	Guarantees offered to the data subject	
16	Steps in the certification process	<ol style="list-style-type: none"> 1. Application 2. Receipt of documents by applicant 3. Self-testing by applicant 4. Applicant sends contract 5. Criteria checks – If criteria not fulfilled, applicant to make changes. If criteria fulfilled, trust mark awarded.
17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification cost)	-
19	Validity	-
20	Revocation mechanism	-
21	Recognition	-
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	-
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	The Euro-Label European Code of Conduct serves as a collective minimum standard.
26	Frequency and means of updates to scheme	-
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	Article 11 of the Euro-Label European Code of Conduct deals with the handling of complaints and out-of-court settlement of litigation.
29	Criticisms	<ul style="list-style-type: none"> • As per the Euro-Label website, the respective internet sites of the French, Spanish, and Italian national operators are inactive. • The Databank Case Study suggests “Firms located in countries with a low share of online sales are less interested in Euro-Label”.
30	Links and references to the scheme	<ul style="list-style-type: none"> • Databank Consulting, Corso Italia, “Case Study- Euro-Label”, <i>E-business Watch</i>, 2004. • Haslinger, Franz, “Euro-label: The

		European Trust mark ”, 2009.
31	Logo	 Germany  Austria  Poland  Italy  France  Spain
32	Website	http://www.euro-label.com
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	Yes, Articles 1 and 2 of the Euro-Label European Code of Conduct .
34	Data collection for specified, explicit and legitimate purposes	Yes, Article 2 of the Euro-Label European Code of Conduct .
35	Adequate, relevant and limited data collection	Yes, Article 2 of the Euro-Label European Code of Conduct .
36	Data accuracy	Yes, Article 2 of the Euro-Label European Code of Conduct .
37	Time and purpose restricted data retention	Yes, Article 2 of the Euro-Label European Code of Conduct .
38	Data is processed under the responsibility and liability of the controller	-
39	Provision for parental consent based	Yes, Article 13 of the Euro-Label European


	processing of personal data of a child below the age of 13	Code of Conduct .
40	Consent requirement for processing of special personal data	-
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Yes, Article 2 of the Euro-Label European Code of Conduct .
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Yes, Articles 2 and 13 of the Euro-Label European Code of Conduct .
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Yes, Article 2 of the Euro-Label European Code of Conduct .
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	-
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	Yes, Articles 1 and 2 of the Euro-Label European Code of Conduct (except from international data transfers)
46	Provision for right of access for the data subject	Yes, Article 2 of the European Code of Conduct.
47	Provision for right to rectification	Yes, Article 2 of the European Code of Conduct.
48	Provision for right to be forgotten and to erasure	-
49	Provision for right to data portability	-
50	Provision for data subject's right to object	Yes, Article 2 of the European Code of Conduct.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Yes, Articles 2 and 10 of the European Code of Conduct
52	Rights in relation to automated processing	-

53	Documentation requirements (Art 28)	-
54	Implementing the data security requirements (Article 30)	-
55	Notification of a personal data breach to the supervisory authority (Article 31)	-
56	Communication of a personal data breach to the data subject (Article 32)	-
57	Data protection impact assessment (Article 33)	-
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	-
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	-

11.11 EUROPRISE

	General criteria for evaluation and comparison of privacy seals	EuroPriSe (European privacy seal)
1	Nature (privacy-oriented/general trust mark)	Privacy seal
2	Country	Germany/Europe
3	Inception	2007 (first seal awarded 2008)
4	Issuing organisation	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Germany
5	Issuer type	Data protection authority
6	Target of scheme	Manufacturers and vendors of IT products and IT-based services. The evaluation subject may be a complete product, a part of a product, a composition of several products or a specific substantial technology. The same applies to IT-based services.
7	Number of certified entities	24 (includes 5 re-certifications)
8	Renewals	5 re-certifications
9	Types of entities that can be certified	Manufacturers and vendors of IT products and IT-based services.
10	Type of beneficiaries	Citizens, business, users, consumers
11	Objective of scheme	According to the website , the EuroPriSe certificate “aims to facilitate an increase of market transparency for privacy relevant products and an enlargement of the market for Privacy Enhancing Technologies and finally an increase of trust in IT”. It seeks to foster “consumer protection & civil rights, trust in IT and privacy by marketing mechanisms” and “promote visibility for privacy compliant and enhancing IT-products and services”.
12	Descriptive summary of scheme	EuroPriSe offers certification to manufacturers and vendors of IT products and IT-based services. The procedure consists of an evaluation of the product or service by accredited legal and IT experts and a validation of the evaluation report by an independent certification body established at the Office of the Data Protection Commissioner of Schleswig-Holstein in Kiel, Germany.
13	Unique selling point	<ul style="list-style-type: none"> • Pan European scheme • Seal issued by an independent third party • Publication of short public report
14	Privacy/data protection elements of the scheme	Data avoidance and transparency, legitimacy of data processing, technical-organisational measures, and data subjects rights. The data protection elements seem extensive, based on European rules on privacy and data protection, contained in particular in Directives 95/46/EC, 2002/58/EC and 2006/24/EC.

15	Guarantees offered to the data subject	<ul style="list-style-type: none"> • Transparency • Legal basis for the processing of personal data • Legal basis for the processing of sensitive personal data • Compliance with General Data Protection principles and duties • Technical-organisational measures: Accompanying measures for protection of the data subject • Rights under the Directive 95/46/EC (right to be informed, right of access, right of correction, right of erasure, right of blocking, right of objection to processing) • Rights under the Directive 2002/58/EC (right to be informed of personal data breaches, right to be informed of security risks, right to confidentiality of communications, right to receive non-itemised bills, right to prevent calling line and/or connected line identification and call forwarding, special rights regarding directories of subscribers to electronic communications services).
16	Steps in the certification process	<ol style="list-style-type: none"> 1. Choose and contact a legal and a technical expert. 2. Discuss evaluation with experts 3. Contact the certification body and schedule a preparatory first meeting 4. Agree on evaluation with experts 5. Apply for certification and conclude a Certification Agreement with the Certification Body 6. Experts conduct evaluation 7. Manufacturer/Service provider hands in <ul style="list-style-type: none"> • <i>Evaluation Report (confidential)</i> compiled by legal and technical expert and approved by manufacturer. • <i>Short Public Report (public)</i> compiled by legal and technical expert and approved by manufacturer.
17	Coverage of international transfers	Sub-set 2.4.2 of the EuroPriSe Criteria 'Transfer to Third Countries' covers this aspect.
18	Costs (i.e., evaluation cost, certification cost)	Expert evaluations are subject to remuneration; fees are individually negotiated by the parties. Validation by certification body is subject to remuneration.
19	Validity	2 years
20	Revocation mechanism	Not clear.
21	Recognition	Positively received by European Data Protection Supervisor (EDPS), the EC Commissioner for Information Society and Media (Viviane Reding).
22	Accredited experts and/or evaluation bodies	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD).
23	Duration and scope of the certification process	Not clear.
24	Number of certified experts and/or bodies	EuroPriSe has around 147 experts in countries such as Argentina, Austria, Croatia, Finland, France, Germany,

		Ireland, Luxembourg, Netherlands, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Taiwan, UK and USA.
25	Regulatory/ compliance standards	EuroPriSe criteria and requirements - based on European rules on privacy and data protection, contained in particular in Directives 95/46/EC, 2002/58/EC and 2006/24/EC.
26	Frequency and means of updates to scheme	According to the website , the scheme is based on European Directives on privacy and data protection and “applied in line with the European jurisdiction and opinions issued by the Art. 29 Data Protection Working Party”. The EuroPriSe criteria were amended in 2010 in response to the amendment of the ePrivacy Directive (2002/58/EC) by the EU Telecoms Reform Package. Editorial changes have also been made. All data is freely available online.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	<ul style="list-style-type: none"> Monitoring by expert during validity period to ensure continuous compliance. Logging of access to personal data and of their processing. Network and transport security. Mechanisms to prevent accidental loss of data; back-up mechanisms and recovery
28	Complaints mechanism	Via website.
29	Criticisms	<ul style="list-style-type: none"> Limited number of certifications.
30	Links and references to the scheme	<ul style="list-style-type: none"> Aced-Félez, Emilio “The EuroPriSe Project: Privacy Seals and the Promotion of Trust”, <i>Proceedings of the International Conference on Information Technologies (InfoTech-2008)</i>, 19 Sept 2008, Vol. 1, pp. 61-60. EuroPriSe, Criteria, https://www.european-privacy-seal.eu/criteria/index.html
31	Logo	
32	Website	https://www.european-privacy-seal.eu/
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	Set 2 of the EuroPriSe criteria deals with legitimacy of data processing. It covers the legal basis of the processing, special requirements relating to the various phases of the processing, compliance with general data protection principles and duties and a number of special types of processing operations.
34	Data collection for specified, explicit and	Sub-set 2.3.1 of the EuroPriSe criteria deals with

	legitimate purposes	purpose-specification and limitation.
35	Adequate, relevant and limited data collection	Sub-set 2.3.2 of the EuroPriSe criteria deals with proportionality.
36	Data accuracy	Sub-set 2.3.3 of the EuroPriSe criteria deals with quality of data.
37	Time and purpose restricted data retention	Sub-set 2.2.4 of the EuroPriSe criteria deals with erasure of data after cessation of requirement.
38	Data is processed under the responsibility and liability of the controller	Implied.
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not found in the EuroPriSe criteria .
40	Consent requirement for processing of sensitive personal data	2.1.2.1 of the EuroPriSe criteria deals with the processing of sensitive data on the basis of explicit consent. It asks: Does the consent (as it is to be expressed by the data subject) meet the requirements of consent? How explicit is the consent?
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	1.2.2.1 of the EuroPriSe criteria deals with transparency and description of the product or service; 4.1.1 of the EuroPriSe criteria covers the data subject's right to be informed. 1.2.2.2 specifically deals with privacy statements.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	4.1.1 of the EuroPriSe criteria deals with the data subject's right to be informed. The criteria do not mention information relating to a child.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Covered under 4.1 of the EuroPriSe criteria - Rights under the Directive 95/46/EC.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	4.1.3 of the EuroPriSe criteria (Right of correction) queries as follows: Are previous recipients of the data informed of the corrections? All of them? Always? Or does this depend on certain matters (like time or purpose)? If so, on what? Is the data subject involved in/consulted on this? 4.1.4 of the EuroPriSe criteria (Right of Erasure) queries: Are previous recipients of the data informed of erasures? All of them? Always? Or does this depend on certain matters (like time or purpose)? If so, on what? Is the data subject involved in/consulted on this?
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the 	Sub-set 4.1.1 of the EuroPriSe criteria comprehensively deals with the data subject's right to be informed in line with Articles 10 and 11 of Directive 95/46/EC. In line with Directive 2002/58/EC, 4.2.1 of the EuroPriSe criteria covers the right to be informed of personal data breaches, and 4.2.2 covers the right to be informed of security risks.


	supervisory authority <ul style="list-style-type: none"> • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	
46	Provision for right of access for the data subject	4.1.2 of the EuroPriSe criteria deals with the right of access.
47	Provision for right to rectification	4.1.3 of the EuroPriSe criteria deals with the right of correction.
48	Provision for right to be forgotten and to erasure	4.1.4 of the EuroPriSe criteria deals with the right of erasure.
49	Provision for right to data portability	Not found.
50	Provision for data subject's right to object	4.1.6 of the EuroPriSe criteria deals with the right to object to processing.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	4.2.6 of the EuroPriSe criteria covers special rights regarding directories of subscribers to electronic communications services. It asks: Can subscribers opt out of direct marketing use of their directory data? If yes: Can they opt out free of charge? How is effect given to such a choice?)
52	Rights in relation to automated processing	3.2.4 of the EuroPriSe criteria covers transparency of automated individual decisions.
53	Documentation requirements (Art 28)	<p>2.3.1 of the EuroPriSe criteria, on purpose-specification and limitation, asks: How is (are) the purpose(s) for which the data are obtained documented?</p> <p>3.1.5 on data protection and security management deals with sustainability of data protection measures, and highlights the following important aspects: policy issues, choice and justification of measures, detailed documentation and checks of measures. 3.1.5.2 queries whether the product documentation provides information on the nature of the data being processed to allow a sufficiently clear classification of data that would enable a user to adopt appropriate security measures. 3.1.5.4 covers with documentation of individual obligations.</p>
54	Implementing the data security requirements (Article 30)	Set 3 of the EuroPriSe criteria deals with technical-organisational measures. 3.1 outlines general duties (preventing unauthorised access to data, programs, premises and devices, logging of processing personal data, network and transport security, mechanisms to prevent accidental loss of data; back-up mechanisms and recovery, data protection and security management, disposal and erasure of data, access control for temporary files, documentation of products

		and services from a customer’s perspective). 3.2 of the EuroPriSe criteria covers technology-specific and service-specific requirements (encryption, pseudonymisation and anonymisation, technical data protection Functionalities required by Directive 2002/58/EC, transparency of automated individual decisions.
55	Notification of a personal data breach to the supervisory authority (Article 31)	The duty to notify competent national authorities as well as individuals concerned of personal data breaches (Article 4 (3) of the ePrivacy Directive) is covered in 4.2.1 of the EuroPriSe criteria .
56	Communication of a personal data breach to the data subject (Article 32)	Covered in 4.2.1 of the EuroPriSe criteria - data subject’s right to be informed of personal data breaches. It asks, “What measures are taken to enable the person or company to inform subscribers or individuals in the case of a personal data breach without delay?” In addition, it asks whether these measures ensure that adversely affected subscribers or individuals are informed about the nature of the personal data breach and the contact points where more information can be obtained. It also asks whether measures to mitigate the possible adverse effects of the personal data breach are recommended to subscribers or users.
57	Data protection impact assessment (Article 33)	No mention of data protection impact assessment. 3.1.5.9 of the EuroPriSe criteria which covers data protection and security audits suggests, “such audits can be carried out by either internal or external experts. Audits will often not only check effectiveness of measures, but also efficiency.” Aspects highlighted here are: regular monitoring of data protection/data security measures, written report and its availability.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	2.5.2 of the EuroPriSe criteria deals with prior checking. Prior checking is also included as element in 3.2.4 which speaks of ensuring transparency of automated individual decisions.
59	Designation of a data protection officer (Article 35(1))	3.1.5.7 of the EuroPriSe Criteria deals with appointment and duties of security officers. Here it asks the following questions: <ul style="list-style-type: none"> • Has an independent Data Protection Officer or Security Officer been appointed in line with national legislation? Does he or she carry out his or her job free of role conflicts and does he or she have the power needed to ensure compliance? • Does he or she conduct audits on a regular basis, in which he or she checks compliance with the relevant security policies, technical and organisational data security measures, and individual obligations?
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	3.1.5.9 of the EuroPriSe Criteria covers data protection and security audit.

11.12 GIGYA'S SOCIALPRIVACY™ CERTIFICATION

	General criteria for evaluation and comparison of privacy seals	Gigya's SocialPrivacy™ Certification
1	Nature (privacy-oriented/general trust mark)	Social privacy certification seal
2	Country	USA. Located in London too.
3	Inception	Launched on 13 December 2012.
4	Issuing organisation	Gigya, Inc.
5	Issuer type	Privately held technology company
6	Target of scheme	Websites, mobile applications
7	Number of certified entities	At launch, four businesses including Martha Stewart Living Omnimedia, LUSH Cosmetics, Finish Line (Run.com), and The Globe and Mail are Gigya SocialPrivacy™ Certification launch partners were expected to implement the SocialPrivacy™ Certification Seal. Gigya's website states that it is "currently providing SocialPrivacy™ Certification regarding Social Login for: Facebook, Twitter, LinkedIn, Google, Yahoo and Windows Live Messenger".
8	Renewals	-
9	Types of entities that can be certified	Companies with websites, mobile applications.
10	Type of beneficiaries	Users of social websites, users of mobile applications.
11	Objective of scheme	To assure users that a business adheres to the highest standard of social data management practices. To create transparency between businesses and consumers when consumers authenticate their online identity via social login.
12	Descriptive summary of scheme	An applicant seeking to be certified by Gigya must comply with its program requirements, which Gigya determines in its sole discretion. Upon satisfactory certification, Gigya provides the applicant with the SocialPrivacy™ Certification seal as evidence of certification. The seal must be displayed on all end user registration and login windows or dialog boxes on an applicant's website or mobile application. It may also be displayed on additional pages of a website and where Social Login or Social Network Data is collected.
13	Unique selling point	<ul style="list-style-type: none"> • Certification of social privacy. • Right to audit scheme participants at any time (even by secret means).
14	Privacy/data protection elements of the scheme	Data protection for social profile data.
15	Guarantees offered to the data subject	Certified entities <ul style="list-style-type: none"> • Will not sell social profile data of users or their

		<p>friends to third parties</p> <ul style="list-style-type: none"> • Will not publicly post to a user's social network account on behalf of a user without the user's explicit permission • Will not send private messages to a user's friend(s) unless prompted by the user. • Will not use personal information obtained via Social Login to send newsletters or promotional emails unless users have opted-in to such notifications.
16	Steps in the certification process	<ul style="list-style-type: none"> • Complete application form • Evaluation of compliance with program requirements by Gigya • Certification
17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification cost)	According to a press report , “Gigya intends to audit publishers that carry its privacy seal... the service will probably cost publishers between \$500 and \$1,000 a month.”
19	Validity	One year. A seal holder must undergo re-certification annually to verify ongoing compliance with the SocialPrivacy™ Certification Program Requirements .
20	Revocation mechanism	Not prescribed in the SocialPrivacy™ Certification Program Requirements or Data Misuse Resolution Policy.
21	Recognition	Gigya’s website suggests it is “currently providing SocialPrivacy™ Certification regarding Social Login for: Facebook, Twitter, LinkedIn, Google, Yahoo and Windows Live Messenger”.
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	Not clear.
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	Gigya’s SocialPrivacy™ Certification Program Requirements , Data Misuse Resolution Policy, Social Network Terms of the SocialPrivacy™ Social Networks .
26	Frequency and means of updates to scheme	Not specified.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	Gigya has a dispute resolution process. Users who suspect any misuse of their social network data in contravention of the Program Requirements may lodge complaints. The user must confirm website or mobile application in question is a “participant property” and a member of the SocialPrivacy™ Certification Program,

		verify that the complaint is a privacy matter related to one of the SocialPrivacy™ Principles and contact the participant first. The scheme participants must provide users with reasonable, appropriate, simple, and effective means to submit complaints, express concerns, or provide feedback regarding its privacy practices. Gigya expects participants to cooperate with its efforts to investigate and resolve non-frivolous privacy complaints, questions, and concerns raised either by users through Gigya's dispute resolution process or Gigya. A participant must comply with any additional requirements set forth in the Data Misuse Resolution Policy.
29	Criticisms	<ul style="list-style-type: none"> • Purely voluntary standard. • Revocation policy not easily available or specified. • The <u>SocialPrivacy™ Certification Program Requirements</u> are not sufficiently detailed; opting to let participants “treat all Participant User Data and Social Network Data in accordance with the posted Privacy Statement in effect at the time of collection”.
30	Links and references to the scheme	<ul style="list-style-type: none"> • Future of Privacy Forum, “Gigya launches SocialPrivacy™ Certification in collaboration with FPF”, 13 December 2013. http://www.futureofprivacy.org/2012/12/13/gigya-socialprivacy-certification/
31	Logo	
32	Website	http://www.gigya.com/
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	<p>The <u>SocialPrivacy™ Certification Program Requirements</u> prohibit seal holders from selling social network data of its users or their friends to third parties.</p> <p>Participants shall treat all participant user data and Social Network Data in accordance with the posted privacy statement in effect at the time of collection unless the participant user otherwise has given explicit permission or unless such use is a result of a non-material change to the privacy statement.</p>
34	Data collection for specified, explicit and legitimate purposes	According to <u>SocialPrivacy™ Certification Program Requirements</u> , seal holders may not use personally identifiable information obtained via social login to send newsletters, promotional emails or any other advertising unless users have opted-in to such notifications.
35	Adequate, relevant and limited data	Participants of scheme must adhere to four prescribed

	collection	criteria on data protection, social publishing, friend protection and email opt-in. See SocialPrivacy™ Certification Program Requirements .
36	Data accuracy	-
37	Time and purpose restricted data retention	Time- no. Purpose - yes.
38	Data is processed under the responsibility and liability of the controller	-
39	Provision for parental consent based processing of personal data of a child below the age of 13	In obtaining any Social Network Data from SocialPrivacy™ Social Networks that include any non-public personally identifiable information for users aged 3-17, the participant must obtain explicit permission.
40	Consent requirement for processing of special personal data	The SocialPrivacy™ Certification Program Requirements prescribe that a participant must get explicit consent from users to do the following: <ul style="list-style-type: none"> • Post to a participant user's social network feed on behalf of the participant user. • Send private messages to a participant user's friends on behalf of the participant user. • Send the participant user emails for marketing or promotional purposes. • Obtaining social network data from socialprivacy™ social networks that includes any non-public PII for participant users aged 13-17.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Scheme participants are required to have an accurate and up-to-date, clear and conspicuous privacy statement that accurately describes how user data is collected, used, displayed, and shared or transferred.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Scheme participants must accurately describe how user data is collected, used, displayed, and shared or transferred in their privacy statement.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	The SocialPrivacy™ Certification Program Requirements prescribe a Dispute Resolution Process.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not specified in the SocialPrivacy™ Certification Program Requirements .
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored 	Not specified in the SocialPrivacy™ Certification Program Requirements .

	<ul style="list-style-type: none"> • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	
46	Provision for right of access for the data subject	Scheme participants must provide users with reasonable, appropriate, simple, and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices.
47	Provision for right to rectification	Scheme participants must provide users with reasonable, appropriate, simple, and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices.
48	Provision for right to be forgotten and to erasure	Not specified in the SocialPrivacy™ Certification Program Requirements .
49	Provision for right to data portability	Not specified in the SocialPrivacy™ Certification Program Requirements .
50	Provision for data subject's right to object	Scheme participants must provide users with reasonable, appropriate, simple, and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	-
52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	Not specified in the SocialPrivacy™ Certification Program Requirements .
54	Implementing the data security requirements (Article 30)	Not specified in the SocialPrivacy™ Certification Program Requirements .
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not specified in the SocialPrivacy™ Certification Program Requirements .
56	Communication of a personal data breach to the data subject (Article 32)	Not specified in the SocialPrivacy™ Certification Program Requirements .
57	Data protection impact assessment (Article 33)	Not specified in the SocialPrivacy™ Certification Program Requirements .
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not specified in the SocialPrivacy™ Certification Program Requirements .
59	Designation of a data protection officer (Article 35(1))	Not specified in the SocialPrivacy™ Certification Program Requirements .


60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	Gigya states that audits of certified businesses are conducted on a regular basis to ensure that requirements are consistently being met. Gigya states in its program requirements that it “reserves the right to audit the participant’s adherence to the Program Requirements at any time”. Such auditing may include: registering via social login on the participant’s properties, opting into and out of marketing or promotional materials sent by participant, “secret” shopping on third party data broker or advertising networks for Social Network Data.
----	---	---

11.13 MARKET RESEARCH SOCIETY (MRS) FAIR DATA MARK

	General criteria for evaluation and comparison of privacy seals	Market Research Society (MRS) Fair Data Mark
1	Nature (privacy-oriented/general trust mark)	Personal data mark
2	Country	UK
3	Inception	January 2013
4	Issuing organisation	Market Research Society (MRS)
5	Issuer type	Research association
6	Target of scheme	Consumer organisations, suppliers of research and data, public/government bodies
7	Number of certified entities	17 organisations
8	Renewals	-
9	Types of entities that can be certified	All organisations – public and private sector – collecting and using personal data.
10	Type of beneficiaries	Customers of consumer organisations, buyers of research and data, supply chain, the public.
11	Objective of scheme	To help consumers recognise who they can trust.
12	Descriptive summary of scheme	According to its website : The Fair Data mark is a consumer facing mark which appears on corporate materials as a guarantee that an organisation meets the Fair Data principles . A Fair Data organisation agrees to: adhere to the Fair Data principles and use the Fair Data mark in all relevant dealings with customers and respondents. As the scheme develops, there will be an audit process conducted by ABC (Audit Bureau of Circulations), to ensure continued compliance.
13	Unique selling point	Targets both public and private sector organisations collecting and using personal data.
14	Privacy/data protection elements of the scheme	Collection and use of personal data. Protection of all respondents from harm - particularly the young and vulnerable.
15	Guarantees offered to the data subject	A Fair Data brochure states: As a Fair Data organisation, you can trust that we will manage and treat your personal data with respect. We will collect, store and manage it in an unbiased and secure way. We will only use your personal data for purposes that we have informed you about and sought your consent for. We will always be transparent about the personal data we collect and how we use it.
16	Steps in the certification process	All Fair Data scheme applicants receive advice from the MRS regarding the Fair Data requirements. MRS company partners or MRS client partners, as organisations that have already signed up corporately to the MRS Code of Conduct

		are therefore committed to the Fair Data principles, can automatically become accredited as a Fair Data organisation. For all other organisations, an initial advisory visit by MRS is required. If the advisory visit has a satisfactory outcome, organisations can undertake a first party assessment to the Fair Data principles. Within the first year, such organisations must also undertake an independent third party audit to verify adherence to the principles. The audit must be undertaken by an MRS approved audit and assessment body. Only those organisations that pass the audit may continue to use the Fair Data mark.
17	Coverage of international transfers	Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. (MRS Data Protection Guidance Document , in conformity with the Data Protection Act 1998 [DPA 1998])
18	Costs (i.e., evaluation cost, certification cost)	<ul style="list-style-type: none"> • Initial advisory visit £1,000 per day. • If organisation fails initial visit and needs another - £500 per day. • Cost of accreditation £350 per year. • Audit fees will be determined on a case-by-case basis.
19	Validity	The accreditation is awarded on an annual basis and is governed by the Fair Data Audit Board which is a tripartite board with representatives from MRS, Audit Bureau of Circulations (the audit partner) and the organisations that are Fair Data accredited.
20	Revocation mechanism	Each year an organisation, that is not an MRS company partner, needs to undertake an audit. The outcome of the audit is managed by the Fair Data Audit Board which will decide if companies can use or continue to use the Fair Data Mark. If a complaint is received that indicates that the Fair Data Principles have been breached, then the relevant organisation is obliged to either submit to an investigation or a third party audit. MRS company partners do not need to undergo an annual audit, as they are already obliged to follow the MRS Code of Conduct which includes all the Fair Data principles. However, should a complaint be received about an MRS company partner, they too would be obliged to have a third party audit.
21	Recognition	-
22	Accredited experts and/or evaluation bodies	The Fair Data Audit Partner is ABC (Audit Bureau of Circulations). This is for all UK based companies. For overseas audits, MRS (in consultation with the Audit Bureau of Circulations)

		must approve any organisations that wish to undertake Fair Data audits (and potentially provide training) before they are able to undertake any Fair Data related activities.
23	Duration and scope of the certification process	The duration of the certification process depends on the size of the organisation. For smaller or centralised organisations which for example have one central data point, have a clear data policy, etc. would most likely need to have one day's initial advisory visit to ensure that they comply with the 10 principles, and the subsequent audit would in all likelihood take several days. The certification lasts for 12 months.
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	MRS's Fair Data principles and the MRS Code of Conduct . The principles support and complement the Data Protection Act 1998, and other standards schemes such as ISO, the US 'Safe Harbor' Framework and the Data Seal initiative. MRS members are expected to abide by the MRS Data Protection Guidance Document .
26	Frequency and means of updates to scheme	Not evident yet, the scheme was launched in 2013.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	In the first instance, complainants are expected to contact the concerned organisation directly. Members and company partners are obliged to assist in the resolution of complaints. MRS has set out a model complaints handling standard for company partners which it will use as a guide to assess whether all reasonable steps have been taken to resolve the complaint before MRS will consider it. If the complainant is dissatisfied with the member's or company partner's response, they may make a formal complaint to MRS. All complaints are initially investigated by the Market Research Standards Board (MRSB). However, all MRS Members may request a disciplinary tribunal, after an initial investigation by the MRSB, and in such instances cases are referred to the MRS Disciplinary Authority . The Authority comprises MRS Fellows and individuals who are independent of both MRS and the market research profession.
29	Criticisms	<ul style="list-style-type: none"> Complaints information is on the main MRS website not on Fair Data website.
30	Links and references to the scheme	<ul style="list-style-type: none"> Gordon, Wendy, "Fair Data – the crocodile dilemma", 7 May 2013 http://www.mrs.org.uk/article/item/735

31	Logo	
32	Website	http://www.fairdata.org.uk/
General data protection regulation requirements under Ch II and III		
33	Fair, lawful, transparent processing of personal data	Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: - at least one of the conditions in Schedule 2* of the Act is met, and - in the case of sensitive personal data, at least one of the conditions in Schedule 3* is also met (MRS Data Protection Guidance Document , in conformity with DPA 1998).
34	Data collection for specified, explicit and legitimate purposes	Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or other purposes (MRS Data Protection Guidance Document , in conformity with DPA 1998).
35	Adequate, relevant and limited data collection	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed (MRS Data Protection Guidance Document , in conformity with DPA 1998).
36	Data accuracy	Personal data shall be accurate and, where necessary kept up to date (with every reasonable step being taken to ensure that data that are inaccurate or incomplete, having regard to the purpose (s) for which they were collected or for which they are being further processed, are erased or rectified) (MRS Data Protection Guidance Document , in conformity with DPA 1998).
37	Time and purpose restricted data retention	Principle 2 of the Fair Data principles states: We will not use personal data for any purpose other than that for which consent was given, respecting customers' wishes about the use of their data. (MRS Data Protection Guidance Document , in conformity with DPA 1998)
38	Data is processed under the responsibility and liability of the controller	Client organisations have the responsibility as data controllers under the 1998 Act to ensure that any data at a personal level passed back from an agency is used solely for the purpose(s) for which the respondent gave their informed consent. (MRS Data Protection Guidance Document) No mention of liability.

39	Provision for parental consent based processing of personal data of a child below the age of 13	The MRS Data Protection Guidance Document only mentions that children have the same rights as adults within the DPA 1998.
40	Consent requirement for processing of special personal data	Principle 1 of the Fair Data principles states: We will ensure that all personal data is collected with customers' consent.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Not covered as such in the MRS Data Protection Guidance Document
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	The MRS Data Protection Guidance Document calls for transparency - ensuring individuals have a very clear and unambiguous understanding of the purpose (s) for collecting the data and how it will be used.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Not specified in the MRS Data Protection Guidance Document , which only mentions: Personal data shall be processed in accordance with the rights of data subjects under the DPA 1998.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not specified in the MRS Data Protection Guidance Document .
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequate decision by the Commission • Any further information necessary to guarantee fair processing 	The MRS Data Protection Guidance Document suggests that “Data subjects are entitled to know the purposes for which the data is held, the data sources, and the category of any others to whom the data may be passed”.
46	Provision for right of access for the data subject	Principle 3 of the Fair Data principles states: We will make sure that customers have access to their personal data that we hold, and that we tell them how we use it.
47	Provision for right to rectification	Not covered as such in the MRS Data Protection Guidance Document .
48	Provision for right to be forgotten and to erasure	Not covered in the MRS Data Protection Guidance Document .
49	Provision for right to data portability	Not covered in the MRS Data Protection Guidance Document .
50	Provision for data subject's right to object	The MRS Data Protection Guidance Document does not specifically mention a right to object. It only states that at “the time that the data is collected, individuals must give their consent to

		<p>their data being collected, and at this time, have the opportunity to opt out of any subsequent uses of the data”.</p> <p>However, the MRS Data Protection Guidance Document does acknowledge the data subject’s right to prevent processing of data for direct marketing, i.e. data subjects have a right to request organisations to cease or not to begin processing his/her personal data for direct marketing purposes.</p>
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not explicitly offered thus in the MRS Data Protection Guidance Document .
52	Rights in relation to automated processing	Not covered in the MRS Data Protection Guidance Document .
53	Documentation requirements (Art 28)	Not covered explicitly in the MRS Data Protection Guidance Document .
54	Implementing the data security requirements (Article 30)	Principle 4 of the Fair Data principles states: We will protect personal data and keep it secure and confidential.
55	Notification of a personal data breach to the supervisory authority (Article 31)	Further, the MRS Data Protection Guidance Document states: data controllers are required to take appropriate steps, including steps of a technical and organisational nature, to protect personal data from accidental or unlawful destruction or accidental loss, alteration or disclosure. Data controllers must have written contracts with processors (e.g. sub-contractors) ensuring the security of the data. This must confirm the subcontractors’ agreement to process personal data in accordance with the data controllers’ instructions and to implement technical and organisational measures equivalent to those required of the data controller.
56	Communication of a personal data breach to the data subject (Article 32)	Not covered in the MRS Data Protection Guidance Document .
57	Data protection impact assessment (Article 33)	<p>The MRS Data Protection Guidance Document suggests that by conducting data protection audits, members will be able to identify data sources within the organisation.</p> <p>Data protection impact assessment is not mentioned.</p>
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not covered in the MRS Data Protection Guidance Document .
59	Designation of a data protection officer (Article 35(1))	The MRS Data Protection Guidance Document advises: there should be one individual who is responsible for data protection (ensuring that the organisations’ responsibilities as a data controller are met), possibly as part of more general


		responsibilities covering data security, and that everyone within the organisation knows who this individual is and where queries on the legislation or subject access requests should be sent.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	<p>The MRS Data Protection Guidance Document advises its members to conduct a yearly audit to ensure that their data protection policies are being fully applied.</p> <p>The Fair Data website specifies. “As the scheme develops, there will be an audit process conducted by ABC (Audit Bureau of Circulations), to ensure continued compliance.”</p>

11.14 MCAFEE SECURE

	General criteria for evaluation and comparison of privacy seals	McAfee SECURE
1	Nature (privacy-oriented/general trust mark)	General trust mark
2	Country	International
3	Inception	Previously known as McAfee “Hacker Safe”, changed to McAfee SECURE in 2008.
4	Issuing organisation	McAfee, Inc.
5	Issuer type	Private company
6	Target of scheme	Websites
7	Number of certified entities	80,000+ websites.
8	Renewals	Daily site scanning, testing for more than 45,000 known vulnerabilities. Automatic renewal at the end of each subscription period.
9	Types of entities that can be certified	Websites, domains and individual IP addresses and pages. Excluded entities include competitors of McAfee, customers convicted of computer or internet related crime, customers in breach of contract with McAfee for more than 60 days, and in any region prohibited from using the service by law.
10	Type of beneficiaries	SECURE customers (Claims to increase online sales conversion by average of 12%), web site customers and visitors.
11	Objective of scheme	To build trust and increase online sales from security conscious shoppers
12	Descriptive summary of scheme	<p>McAfee conducts daily vulnerability scanning of member websites, mimicking the process through which hackers would search for vulnerabilities. The website owner is alerted to any vulnerability found and given technical support in addressing these vulnerabilities.</p> <p>McAfee SECURE trust marks are “live” and display the current date (following the daily vulnerability scan), clicking on the seal takes the user to the dedicated verification page (hosted by McAfee) featuring the company name of the online merchant.</p> <p>According to its website, “The McAfee SECURE standard is an aggregate of industry best practices, designed to provide a level of security that an online merchant can reasonably achieve to help provide consumers with better protection when interacting with websites and online shopping.”</p>

13	Unique selling point	Known brand, world's largest dedicated online security company. Daily website vulnerability scanning
14	Privacy/data protection elements of the scheme	The scheme focuses on information security and makes no claims regarding the intentional information processing practices of any participating merchants.
15	Guarantees offered to the data subject	McAfee makes no warranty or claim of any kind.
16	Steps in the certification process	McAfee first conducts a vulnerability scan. After the website addresses any issues raised, it can start using the trust mark. The vulnerability scan is then conducted daily. The process may thus be considered as ongoing. No additional software or hardware is required. McAfee conducts periodic tests for accidental practices that can lead to bad publicity and lost consumer confidence.
17	Coverage of international transfers	Not stated.
18	Costs (i.e., evaluation cost, certification cost)	The McAfee SECURE Scan costs between €366 p.a. for a single domain or IP address on a one year contract, to €56 per domain or IP as part of a bundle of 128 or more, on a three year contract (excluding VAT). There is a €100 start-up cost. Access to McAfee SECURE logos ranges from €163 for 1-2 logos served per day on a one year contract, to volume discounts of €12 for more than 2000 logos. An example calculation of daily scanning of two domain names, and showing 6,000 logos per day equalled €1,270 for one year. There are potential overage charges.
19	Validity	Live trust marks will display today's date. Sites that use McAfee SECURE service must maintain their security status to be eligible to display the trust mark. There is automatic renewal at the end of each subscription period.
20	Revocation mechanism	Members are informed of vulnerabilities detected during the vulnerability scan and must maintain a level of security in order to continue to display the trust mark. It is not clear what level of vulnerability would prevent the display of mark. McAfee will discontinue the serving of the SECURE image, if any customer website, or other device that is being scanned in connection with the services, fails to pass McAfee's vulnerability audits for a period of 72 hours or longer.
21	Recognition	McAfee has won several security industry awards, but not specifically for the SECURE

		trust mark.
22	Accredited experts and/or evaluation bodies	Businesses can partner with McAfee to sell McAfee SECURE services and Payment Card Industry (PCI) Certification to their customers. This includes affiliate and global reseller programmes. Partners are divided into e-commerce design and platform providers, hosting companies, payment gateways, and strategic partners.
23	Duration and scope of the certification process	After an initial scan, customer websites may be able to display McAfee SECURE trust mark in as little as a day.
24	Number of certified experts and/or bodies	Not stated.
25	Regulatory/ compliance standards	McAfee is annually certified to PCI level One security standard: https://www.pcisecuritystandards.org/document/s/pci_dss_v2.pdf Vulnerability scanning is part of certification for the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes-Oxley Act (SOX), ISO17799 (Information Security Guidelines and Principles), and the Statement on Auditing Standards (SAS) No. 70, Service Organizations.
26	Frequency and means of updates to scheme	There are daily updates to the vulnerabilities database. No information provided on the frequency of changes to programme requirements.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	<ul style="list-style-type: none"> • McAfee SiteAdvisor software highlights McAfee SECURE sights in search results. • Addition to certified McAfee SECURE Merchants Directory: http://www.mcafee.com/apps/mcafeeseecure/merchant-directory.aspx • Daily security scans for vulnerabilities and support from security professionals. • Automatic revocation of seal following vulnerability scan may act as a signal of sites vulnerable to attack.
28	Complaints mechanism	By email to compliance@mcafee.com
29	Criticisms	<ul style="list-style-type: none"> • Past failure to including particular types of vulnerabilities (cross-site scripting errors). • Security seal information page largely advertising for McAfee. • Charging per seal download/view. • SECURE service users criticised the merchants' directory/shopping portal for directing their customers to their

		<ul style="list-style-type: none"> competition. The SiteAdvisor effects upon search rank are seen as pressure to pay for a McAfee seal.
30	Links and references to the scheme	<ul style="list-style-type: none"> Goodin, Dan, "McAfee 'Hacker Safe' cert sheds more cred", <i>The Register</i>, 29 April 2008. http://www.theregister.co.uk/2008/04/29/mcafee_hacker_safe_sites_vulnerabl_e/ Trust Guard, "Trust Guard vs. Hacker Safe", http://www.trust-guard.com/Hacker-Safe-s/42.htm Goodin, Dan, "McAfee, Trust Guard certifications can make websites less safe", <i>ARS Technica</i>, 6 Oct 2012 http://arstechnica.com/security/2012/10/mcafee-trust-guard-certifications-can-make-websites-less-safe/
31	Logo	
32	Website	http://www.mcafee.com/us/mcafeesecure/products/mcafee-secure.html
General data protection regulation requirements under Ch II and III		
33	Fair, lawful, transparent processing of personal data	The McAfee Secure seal is primarily an information security seal, based upon a scan of website technical vulnerabilities. Neither this scan, nor the terms of use make any reference to personal data processing activities. The only element of data protection covered by this seal is the security requirements to prevent unauthorised processing.
34	Data collection for specified, explicit and legitimate purposes	Not stated.
35	Adequate, relevant and limited data collection	Not stated.
36	Data accuracy	Not stated.
37	Time and purpose restricted data retention	Not stated.
38	Data is processed under the responsibility and liability of the controller	Not stated.
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not stated.
40	Consent requirement for processing of special personal data	Not stated.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Not stated.
42	Intelligible, clear information, communication relating	Not stated.


	to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Not stated.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not stated.
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and level of protection afforded by that third country or international organisation by reference to an adequacy decision of the Commission • Any further information necessary to guarantee fair processing 	Not stated.
46	Provision for right of access for the data subject	Not stated.
47	Provision for right to rectification	Not stated.
48	Provision for right to be forgotten and to erasure	Not stated.
49	Provision for right to data portability	Not stated.
50	Provision for data subject's right to object	Not stated.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not stated.
52	Rights in relation to automated processing	Not stated.
53	Documentation requirements (Art 28)	Not stated.
54	Implementing the data security requirements (Article 30)	In Europe, being a member of McAfee SECURE (sold through their partner B2U.NL) is promoted as providing a strong legal case for complying with the security requirements of Directive 95/46/EC to maintain security and prevent unauthorised processing. http://www.hackersafe.eu/en/mcafee-secure/privacy-regulation/
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not stated.
56	Communication of a personal data breach to the data subject (Article 32)	Not stated.
57	Data protection impact assessment (Article 33)	Not stated.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not stated.
59	Designation of a data protection officer (Article 35(1))	Not stated.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor	Not stated.

	obligations	
--	-------------	--

11.15 PRIVACYMARK SYSTEM

	General criteria for evaluation and comparison of privacy seals	PrivacyMark System (Japan)
1	Nature (privacy-oriented/general trust mark)	Privacy mark
2	Country	Japan
3	Inception	1 April 1998
4	Issuing organisation	Japan Information Processing (JIPDEC) administers the PrivacyMark system; Conformity assessment bodies accredited by JIPDEC issue the mark.
5	Issuer type	Non-profit public corporation established under Japanese law in 1967 to promote computer technologies and ensure the security of information systems. Accreditation body.
6	Target of scheme	Private enterprises based in Japan.
7	Number of certified entities	15, 667 (as at March 2013)
8	Renewals	A two-year extension can be applied for after the two year validity period. Renewal may be applied for every two years thereafter. A renewal application must be made between 3 to 4 months prior to the termination of validity.
9	Types of entities that can be certified	Private enterprises based in Japan. Overseas enterprises can apply if they are registered as a Japanese branch under Japanese laws and hold personal information separate from their foreign parent company.
10	Type of beneficiaries	Consumers, businesses.
11	Objective of scheme	To enhance consumer awareness of personal information protection and to provide entities with an incentive to win social trust from consumers and business partners.
12	Descriptive summary of scheme	According to its website , the PrivacyMark is “a system set up to assess private enterprises that take appropriate measures to protect personal information”. Private enterprises are granted the right to display the PrivacyMark in the course of their business activities. Conformity assessment bodies receive applications, screen them, conduct an in situ assessment and certify conformity.
13	Unique selling point	The PrivacyMark may be displayed on storefronts, contracts, manuals, public relations materials, envelopes, letter papers, business cards and websites.
14	Privacy/data protection elements of the scheme	Personal information protection.
15	Guarantees offered to the data subject	The PrivacyMark is intended to guarantee that appropriate protective measures for personal

		information have been adopted by an organisation.
16	Steps in the certification process	<ol style="list-style-type: none"> 1. Prepare application forms 2. Application 3. Application document screening 4. On site assessment (operations and security safeguards) 5. Accreditation notice and PrivacyMark Use Agreement 6. Changes in reporting matters.
17	Coverage of international transfers	Protection of personal information.
18	Costs (i.e., evaluation cost, certification cost)	The application fee for small businesses is ¥300, for medium businesses is ¥600 and for large businesses is ¥1,200. Renewals for a small business costs ¥220, a medium business pays ¥ 450 and a large business pays ¥ 900.
19	Validity	Two years.
20	Revocation mechanism	A mark may be revoked for violation of the prescribed conditions for handling personal information. The revocation procedure is prescribed in the agreement for the utilisation of the mark.
21	Recognition	The Chinese Dalian Software Industry Association (DSIA) and JIPDEC signed a mutual recognition agreement on 19 June 2008 that both parties will recognise entities accredited to meet requirements of DSIA's PIPA or JIPDEC's PrivacyMark system. JIPDEC also has a mutual recognition programme with the Korea Association of Information and Telecommunication (KAIT).
22	Accredited experts and/or evaluation bodies	Number of assessment bodies – 18.
23	Duration and scope of the certification process	Not clear.
24	Number of certified experts and/or bodies	Number of assessor training bodies -3; number of assessors – 1,232
25	Regulatory/ compliance standards	JIS Q 15001:2006 (Japanese Industrial Standard for Personal Information Protection management systems Requirements). This standard is based on the eight OECD principles and the core of the EU Directive 95/46/EC.
26	Frequency and means of updates to scheme	The JIPDEC Secretariat periodically assesses the system and asks the PrivacyMark System Committee to review any issues which then results in modification of standards and regulations. The Secretariat also conducts an annual survey via a survey company, reviews results and takes remedial action. The Secretariat holds an Assessment Body Meeting every two months to share information and review operations and procedures.

27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	Periodic conformity audits.
28	Complaints mechanism	Private enterprises, personal information subjects and consumers can contact JIPDEC with complaints relating to the operation of the PrivacyMark System.
29	Criticisms	<ul style="list-style-type: none"> Counterfeiting concerns
30	Links and references to the scheme	<ul style="list-style-type: none"> Storz, Cornelia, “Private solutions to uncertainty in Japanese electronic commerce”, in Cornelia Storz and Andreas Moerke (eds.), <i>Competitiveness in New Industries</i>, pp 75-102. Miyashita, Hiroshi, “The evolving concept of data privacy in Japanese law”, <i>International Data Privacy Law</i>, Vol. 1, No. 4, 2011, pp. 229-238
31	Logo	
32	Website	http://privacymark.org/
General data protection regulation requirements under Ch II and III		
33	Fair, lawful, transparent processing of personal data	The JIS Q 15001:2006 Guidelines prescribe that a business entity shall acquire personal information legally and fairly.
34	Data collection for specified, explicit and legitimate purposes	The JIS Q 15001:2006 Guidelines prescribe that a business entity, when acquiring personal information, shall identify the purpose of use as much as possible within the scope necessary for the achievement of the purpose.
35	Adequate, relevant and limited data collection	The JIS Q 15001:2006 Guidelines prescribe that the acquisition of personal information must, upon identifying the usage purpose as specifically as possible, be limited to the range necessary for achieving the purpose.
36	Data accuracy	The JIS Q 15001:2006 Guidelines prescribe that the business entity shall control personal information correctly in the state of up-to-date within the scope necessary for the achievement of the purpose of use.
37	Time and purpose restricted data retention	The JIS Q 15001:2006 Guidelines suggest that procedures for determining the retention period of

		personal information shall be stipulated and retention periods shall be determined in accordance with predetermined procedures.
38	Data is processed under the responsibility and liability of the controller	Not prescribed explicitly in this manner.
39	Provision for parental consent based processing of personal data of a child below the age of 13	In regards to consent, the JIS Q 15001:2006 Guidelines prescribe that if the person is a child, consent of the legal representative, etc. is also required in relation to the handling of personal information.
40	Consent requirement for processing of special personal data	The JIS Q 15001:2006 Guidelines contain a restriction on the acquisition, use and provision of specific subtle personal information. The Guidelines prescribe that a business entity shall not acquire, use or provide 'specific subtle' personal information, except when the person consents explicitly to the acquisition, use or provision of personal information, or if any of prescribed provisory clauses in 3.4.2.6 of the Guidelines can be applied.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	<p>Though the JIS Q 15001:2006 Guidelines outline requirements for 'Personal information protection policy', they do not mention the term 'transparent'. However, the Guidelines suggest that the policy must be recognisable "to human senses" and "available to general people". When published on the website, the Guidelines recommend, linking to it from the first page.</p> <p>The Guidelines further prescribe that a business entity, when the acquired personal information can be applied to the personal information subject to disclosure, shall place the following items regarding the personal information subject to disclosure in a readily accessible condition to the person (including when the response is made with no delay at the request of the person).</p>
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	The JIS Q 15001:2006 Guidelines suggest that the personal information protection policy should be recognisable "to human senses" and is "available to general people".
43	Existence of procedures and mechanisms for exercising the rights of the data subject	The JIS Q 15001:2006 Guidelines have a specific section on 'rights of the person concerning personal information'. A business must entity respond to requests for disclosure etc. of personal information subject to prescribed requirements. The Guidelines prescribe the procedures to meet requests for disclosure and others. They also prescribe that a business entity must establish and maintain the procedure to implement proper and prompt actions when receiving complaints and queries about the handling of personal information

		and the personal information protection management system.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	The JIS Q 15001:2006 Guidelines prescribe that after a correction is made, a business entity shall inform the person of the effect and the content without delay and when determined that a correction was not made, shall inform the person of the effect and explain the reason without delay.
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	The JIS Q 15001:2006 Guidelines prescribe: The business entity, when the acquired personal information can be applied to the personal information subject to disclosure, shall place the following items regarding the personal information subject to disclosure in a readily accessible condition to the person (including when the response is made with no delay at the request of the person): <ol style="list-style-type: none"> a) Name or designation of the business entity, b) Name or title, section and the contact of personal information protection manager (or the agent), c) Purpose of use of all of the personal information subject to disclosure (except when a) to c) of 3.4.2.5 can be applied), d) The other party to whom for a complaint on the handling of the personal information subject to disclosure is filed, e) When the business entity is the target business entity of an entity authorized under Clause 1 of Article 37 of Act on the protection of personal information (Law No. 57, 2003), designation of the authorised personal information protection organisation and the other party for applying for solution of the complaints, and f) Procedures to meet requests for disclosure etc
46	Provision for right of access for the data subject	The JIS Q 15001:2006 Guidelines call for procedures for “approving access to the person to be provided”.
47	Provision for right to rectification	A person may request correction of content, addition or deletion of personal information.
48	Provision for right to be forgotten and to erasure	A person may request deletion, stopping use, erasing, and provision of personal information to third parties.
49	Provision for right to data portability	-
50	Provision for data subject’s right to object	Not explicitly expressed as such.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	The JIS Q 15001:2006 Guidelines state that business enterprises must obtain the consent of that person in relation to direct marketing. Businesses have an obligation to give notification of the acquisition method, including details on the source of personal information and how it was acquired.

52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	<p>The JIS Q 15001:2006 Guidelines prescribe: The business entity shall describe in writing the following elements which become the basic of personal information protection management system;</p> <ul style="list-style-type: none"> a) Personal information protection policy, b) Internal regulations, c) Plans, and d) Record required by the Standard and record which the business entity judges that it is necessary for implementing the personal information protection management system. <p>The Guidelines also prescribes that the entity shall establish, implement and maintain the procedure for controlling all documents required by the Standard.</p>
54	Implementing the data security requirements (Article 30)	The JIS Q 15001:2006 Guidelines devote a section to security control measures and specify that a business entity shall take the necessary and appropriate measures to prevent leakage, loss or damage and for other control of security of personal information, according to the risk of the personal information to be handled.
55	Notification of a personal data breach to the supervisory authority (Article 31)	The JIS Q 15001:2006 Guidelines prescribe that if leakage, loss or damage of personal information takes place, the business entity must promptly report the causes and the measures to the relevant organisations.
56	Communication of a personal data breach to the data subject (Article 32)	The JIS Q 15001:2006 Guidelines prescribe that if leakage, loss or damage of personal information occurs, the business entity must inform the information subject promptly of the content of the personal information when the leakage, loss or damage of personal information occurred, or place the person in a readily accessible condition about the content. The entity must state the facts, causes and measures publicly and in a timely manner to prevent secondary damages and the recurrence of such cases.
57	Data protection impact assessment (Article 33)	Only periodic conformity audits specified.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	The JIS Q 15001:2006 Guidelines prescribe that the business entity shall appoint a fair and objective personal information protection auditor within the business and give the auditor the responsibility and authority of executing and reporting audits independent of other


		responsibilities. The auditor directs the audit and prepares the audit report.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	The JIS Q 15001:2006 Guidelines prescribe: The business entity shall periodically audit the conformity status of the personal information protection management system to the Standard and the operation status of the personal information protection management system.

11.16 PRIVO PRIVACY CERTIFIED

	General criteria for evaluation and comparison of privacy seals	PRIVO Privacy Certified (Previously PRIVO Membership Seal of Approval/Privacy Assurance Program)
1	Nature (privacy-oriented/general trust mark)	Privacy seal
2	Country	United States
3	Inception	PRIVO was established in 2001, the Privacy Assurance program was launched in 2003.
4	Issuing organisation	Privacy Vaults Online, Inc, doing business as PRIVO
5	Issuer type	Private company.
6	Target of scheme	Websites directed at children under 13 or who reasonably believe that they collect personal information from children under 13.
7	Number of certified entities	26 member websites (for both Privacy Certified and PrivoLock)
8	Renewals	Not stated – Quarterly self-evaluation and “periodic” unannounced checks.
9	Types of entities that can be certified	Private company websites.
10	Type of beneficiaries	Member companies, Parents of children under 13, children.
11	Objective of scheme	According to its website , “PRIVO is the first and only infomediary service to be recognized by the Federal Trade Commission (FTC) . The PRIVO Privacy Assurance Program was approved as a Safe Harbor provider under the Children’s Online Privacy Protection Act (COPPA) in August 2004. Online businesses/operators are deemed in compliance if the operator complies with Commission approved self-regulatory guidelines. The posting of a PRIVO Program Seal signals to consumers, your partners, advertisers, as well as government, that your site meets the COPPA guidelines.”
12	Descriptive summary of scheme	PRIVO Privacy Certified is a privacy seal focused upon websites collecting and processing information on children, and particularly children under the age of 13. PRIVO has been recognised by the US Federal Trade Commission as an independent certifier (Safe Harbor) for compliance with COPPA. Award of a Privacy Certified Seal demonstrates that the website has reached or surpassed the standards of COPPA.
13	Unique selling point	<ul style="list-style-type: none"> Federal Trade Commission recognised independent certifier of companies certifying compliance with COPPA. Posting a PRIVO Program Seal indicates that a site meets COPPA guidelines.

		<ul style="list-style-type: none"> PRIVO provides consulting services to advise organizations how to meet these compliance requirements. Additionally, safety assurance and privacy certification services are also provided via its FTC approved Safe Harbor Privacy Assurance Program Seal as confirmation that the web site has met the guidelines of COPPA.
14	Privacy/data protection elements of the scheme	See previous item.
15	Guarantees offered to the data subject	Certified sites are compliant with COPPA.
16	Steps in the certification process	<p>Companies conduct initial self-evaluation of website's information collection and disclosure practices. PRIVO conducts an independent review to check for consistency in the self-evaluation form and privacy policy. The independent review has three steps. One, a comparison of self-evaluation form and posted privacy policy; two, a review of the website against the evaluation form and privacy policy, and three, a review of the website's collection and use practices. This involves submitting fictitious personal information and tracking the use of that seeded information.</p> <p>Before becoming a member, the website must make all modifications PRIVO deems necessary for compliance to its website in accordance with the program requirements and COPPA. PRIVO assists member companies in altering or drafting a meaningful privacy policy to assist the members in complying with the program requirements.</p>
17	Coverage of international transfers	Not stated. Members are US companies.
18	Costs (i.e., evaluation cost, certification cost)	Not stated.
19	Validity	Compliance monitoring includes initial and annual self-evaluation, quarterly and periodic unannounced monitoring reviews, and community monitoring reviews.
20	Revocation mechanism	According to itself , "If PRIVO determines that a violation of the requirements has occurred, the member is informed of such violation and the corrective actions that must be taken to bring the member's website into compliance. Failure to take corrective actions can result in a number of consequences including removal from the Privacy Assurance Program and referral to the appropriate government agency." Further, "If PRIVO determines, after a thorough investigation into a member's information practices, that a member has violated its posted privacy policy or any of the requirements described above, PRIVO may refer such members to the Federal Trade Commission for possible unfair and deceptive trade practices."

21	Recognition	The PRIVO privacy assurance program was approved as a Safe Harbor provider by the Federal Trade Commission (FTC) under COPPA in August 2004. This signifies Commission approval of self-regulation guidelines.
22	Accredited experts and/or evaluation bodies	None stated.
23	Duration and scope of the certification process	The certification process includes self-evaluation, review of the privacy policy and determination of where and how personal data is collected on the website and investigation into the actual processing of personal data.
24	Number of certified experts and/or bodies	None stated.
25	Regulatory/ compliance standards	The FTC considers that the standards of the PRIVO Privacy Certification signify compliance with (or reaching higher standards than) the Children's Online Privacy Protection Act (1999, United States)
26	Frequency and means of updates to scheme	Not stated.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	Can be integrated with the PrivoLock system a proprietary verifiable parental consent mechanism.
28	Complaints mechanism	No specific contact details are provided for complaints or dispute resolution other than general info@privo.com . The Privacy Certification requires that "All member companies must provide the parent and child with a reasonable and effective means to submit complaints that they may have about the member company's information practices. The Privacy Assurance program also offers the parent and child the opportunity to submit complaints about any member company website directly to the Privacy Assurance Program. A Representative of the Privacy Assurance Program handles all complaints immediately. The Privacy Assurance Program maintains a record for three years of all complaints."
29	Criticisms	<ul style="list-style-type: none"> • A Galexia study in 2009 found that four out of nine then listed members did not display a working seal. • Program requirements are not displayed on the PRIVO website. • Blurring between Privacy Certified and PRIVO Lock schemes. • If COPPA requirement is legally mandatory, then what is the relevance of the seal? • No information available on PRIVO's 'community monitoring reviews'.
30	Links and references to the scheme	<ul style="list-style-type: none"> • PRIVO's, "Request for Safe Harbor Approval" 3 March 2004. http://www.ftc.gov/os/2004/04/privoapp.pdf

		<ul style="list-style-type: none"> Federal Trade Commission, “Application of Privo, Inc., Children’s Online Privacy Protection Rule Safe Harbor Program” 29 July 2004. http://www.ftc.gov/os/2004/08/040802privoleter.pdf Gasca, Peter, “Why You Need to Consider Children's Privacy” <i>Inc.com</i>, 3 February 2013. http://www.inc.com/peter-gasca/why-kids-are-a-threat-to-your-business.html Connolly, Chris, “Privacy White Lists - Don't be Fooled (2009)”, 2 June 2009. http://www.galexia.com/public/research/assets/privacy_white_lists_2009/ Rubenstein, Ira, “Privacy and Regulatory Innovation: Moving beyond voluntary codes”, <i>I/S A Journal of Law and Policy for the Information Society</i>, Vol. 6, 2011, p. 356. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275
31	Logo	
32	Website	http://www.privo.com/index.htm
General data protection regulation requirements under Ch II and III		
33	Fair, lawful, transparent processing of personal data	If the independent review by PRIVO identifies unlawful processing of personal data, this becomes a ground for revocation of the seal and referral to appropriate authorities.
34	Data collection for specified, explicit and legitimate purposes	PRIVO requires that, “A privacy policy will be posted on the homepage of a member company website and provide a link to such privacy policy at each point within the website where personal information is collected.”
35	Adequate, relevant and limited data collection	PRIVO requires that, “The child’s participation in an activity will not be conditioned on the child’s disclosure of more personal information than is reasonably necessary for the activity.”
36	Data accuracy	PRIVO requires that, “Member companies will maintain the confidentiality, security and integrity of the personal information they collect from children.”
37	Time and purpose restricted data retention	Not stated.
38	Data is processed under the responsibility and liability of the controller	Full contact details of member company must be displayed clearly. Members must appoint a program representative for the website, responsible for overseeing compliance.
39	Provision for parental consent based processing of personal data of a child below the age of 13	PRIVO requires that notice is provided to the child's parent about the website information practices and

		<p>prior verifiable consent will be obtained before collecting personal information from children. The child's parents must be given the choice to consent to the collection and use of their child's information for internal use by the website and the parent must be given the opportunity to elect not to have their child's personal information disclosed to third parties.</p> <p>Members must provide a mechanism for obtaining prior parental consent, which must be reasonably calculated in light of current technology that the person giving consent is the child's parent. Suitable mechanisms include postal consent form, requiring a credit card, calling a toll-free telephone number, or using the PrivoLock system. First name and online contact information of a child does not require parental consent for collection.</p> <p>For the purposes of the PRIVO seal, a 'child' is a person of 12 years or younger.</p>
40	Consent requirement for processing of special personal data	Certification is premised on parental consent for the processing of any data belonging to a child under 13. However, no specific mention of special personal data.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	PRIVO requires that, "A privacy policy will be posted on the homepage of a member company website and provide a link to such privacy policy at each point within the website where personal information is collected."
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	PRIVO requires that, "Notice will be provided to the child's parent about the website information practices and prior verifiable consent will be obtained before collecting personal information from children."
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Not specifically stated.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not specifically stated.
45	<p>Provision of information to data subject:</p> <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation on the level of protection afforded by that third country international organisation by reference to an adequacy decision by the Commission 	<p>Members must post a visible privacy policy link on their homepage and any page where they collect personal data. This must be clear and understandable, and contain the following information: member contact information, types of personal information collected, use of personal information, disclosure of personal information, control over personal information, restrictions on information collection, access to information, and questions and complaints.</p> <p>PRIVO requires that, "The parent will be provided with access to their child's personal information and be given the opportunity to delete the information and opt-out of future collection or use</p>


	<ul style="list-style-type: none"> Any further information necessary to guarantee fair processing 	<p>of the information.”</p> <p>PRIVO requires that, “Member companies must provide the parent and the child with a means to submit questions or complaints that they may have about a member company’s information practices. If the parent or child is not satisfied with the response they receive from the member company, the Privacy Assurance Program offers parents with assistance with resolving those complaints. Such assistance may include contacting the member company directly to investigate the complaint and finding a resolution to the parent or child’s concern or requiring a representative of the member company to participate in the Privacy Assurance Programs alternative dispute resolution services. In both cases, a trained member of the Privacy Assurance Program staff administers the process.”</p> <p>No requirement for information on rights to complain to supervisory authorities, transfers to third countries, or rights of erasure and rectification.</p>
46	Provision for right of access for the data subject	PRIVO requires that, “The parent will be provided with access to their child’s personal information and be given the opportunity to delete the information and opt-out of future collection or use of the information.”
47	Provision for right to rectification	Not stated.
48	Provision for right to be forgotten and to erasure	PRIVO asks member companies to provide parents with access to their child’s personal information and the opportunity to delete the information and opt-out of future collection or use of the information.
49	Provision for right to data portability	Not stated.
50	Provision for data subject’s right to object	PRIVO asks member companies to provide parents with access to their child’s personal information and the opportunity to delete the information and opt-out of future collection or use of the information. It also requires that a child’s participation in an activity is not be conditioned on the child’s disclosure of more personal information than is reasonably necessary for the activity.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Direct marketing is not specifically addressed.
52	Rights in relation to automated processing	Automated processing is not specifically addressed.
53	Documentation requirements (Art 28)	PRIVO requires that a privacy policy is posted on the homepage of a member company website and a link provided to such privacy policy at each point within the website where personal information is collected.
54	Implementing the data security requirements	PRIVO requires that member companies maintain

	(Article 30)	the confidentiality, security and integrity of the personal information they collect from children.
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not stated.
56	Communication of a personal data breach to the data subject (Article 32)	Not stated.
57	Data protection impact assessment (Article 33)	Not stated.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not stated.
59	Designation of a data protection officer (Article 35(1))	Member companies must designate a representative with responsibility for compliance with the program requirements.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	PRIVO conducts period investigations of members, including seeding fictional personal information onto member websites and monitoring the processing of this data.

11.17 SERIEDAD ONLINE

	General criteria for evaluation and comparison of privacy seals	Seriedad Online
1	Nature (privacy-oriented/general trust mark)	General trust mark certifying quality in contents and security in personal data management.
2	Country	Spain
3	Inception	-
4	Issuing organisation	Seriedad Online
5	Issuer type	Private sector organisation
6	Target of scheme	Private sector organisations
7	Number of certified entities	28
8	Renewals	-
9	Types of entities that can be certified	Private sector organisations
10	Type of beneficiaries	Consumers
11	Objective of scheme	To certify member companies as complying with a code of ethical conduct, the Spanish Organic Law on Data Protection (Data Protection Act, Act 15/1999 of December 13, Protection of Personal Data), and Law of Services of the Information Society and Electronic Commerce (LSSICE, Law 34/2002 of July 11 effective from October 2003).
12	Descriptive summary of scheme	Seriedad Online certifies through audits: <ul style="list-style-type: none"> • The security of commercial transactions (for shops) having formally appointed and notified the Data Protection Agency (DPA) who is responsible for its customers' personal data and the data of the owner of the company. • The professionalism and commercial seriousness (member companies voluntarily sign an ethical code of conduct). • The quality of digital content, which are certain and prepared by competent professionals. • Commercial communications (anti-SPAM). • An appropriate protocol for claims.
13	Unique selling point	Certifies both security and data protection.
14	Privacy/data protection elements of the scheme	See Chapters 2-5 (Articles 1-11) of the Seriedad Ethical Code of Conduct .
15	Guarantees offered to the data subject	-

16	Steps in the certification process	<ol style="list-style-type: none"> 1) Application for certification: when the quotation is accepted, the client requests the security seal. In this phase, the client fills out the preliminary information and the evaluation questionnaire, reviews and signs the code of ethical conduct, provides all the data necessary to the certification process. 2) Review of the documentation provided by the client, study the rules applicable to the specific market sector, and registration of the company in the public registry (APD – Data Protection Agency). 3) Audit certification and presentation of the relevant report. 4) Implementation of corrective actions (if required) for full adaptation to the rules. 5) Review of corrective actions provided and completion of the certification. 6) Grant of the certificate and the seal of quality. 7) Publication on the Seriedad Online website as a certified company.
17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification cost)	<p>The cost of joining Seriedad Online varies for each company based on parameters such as size of the company, the type of data it handles, and the sector in which it operates.</p> <p>The trust mark has an €100 annual fee (main website), and €50 annual fee (additional websites)</p>
19	Validity	12 months.
20	Revocation mechanism	-
21	Recognition	-
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	<p>The certification process is specific to each area of the web and of the business sector where the applicant operates, and is characterised by:</p> <ul style="list-style-type: none"> • An audit by Seriedad Online. This is a comprehensive audit of each and every section of the applicant’s website, in order to complete the full adaptation (including not only textual information to users, but also organisational, technical and legal) to the regulations on electronic commerce and data protection.

		<ul style="list-style-type: none"> A formal and detailed process of adaptation to the standards mandated by the Data Protection Act (LOPD) and the LSSICE law. <p>The sign of a detailed and precise commitment to comply with the Ethical Code of Conduct. The Ethical Code of Conduct includes aspects of claims management, business communication (sending of advertising: the fulfillment of certain requirements in relation to the promotional activity that takes place on the Internet, such as spam), break procedure and/or modification of data, consent, and so on.</p>
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	Standards set by the Spanish Data Protection Act (LOPD) and the LSSICE.
26	Frequency and means of updates to scheme	Not clear.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	Consumers may file complaints with Seriedad Online if the provider carries its Trust mark, Seriedad Online will handle (entirely free) the claim and actively intermediate to reach a satisfactory agreement and act to ensure the interests of the claimant. Consumers may also file complaints with Seriedad Online for providers not belonging to its system.
29	Criticisms	-
30	Links and references to the scheme	-
31	Logo	
32	Website	http://www.seriedadonline.es
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	Yes, see Articles 1 and 4 of the Ethical Code of Conduct .
34	Data collection for specified, explicit and legitimate purposes	Yes, see Article 4 of the Ethical Code of Conduct .
35	Adequate, relevant and limited data collection	Yes, see Article 4 of the Ethical Code of Conduct .
36	Data accuracy	Yes, see Article 4 of the Ethical Code of Conduct .
37	Time and purpose restricted data retention	Yes, see Article 4 of the Ethical Code of Conduct .
38	Data is processed under the responsibility and liability of the controller	Yes, see Articles 6-10 of the Ethical Code of Conduct .
39	Provision for parental consent based	-


	processing of personal data of a child below the age of 13	
40	Consent requirement for processing of special personal data	Yes, see Article 5 of the Ethical Code of Conduct .
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Yes, see Article 5 of the Ethical Code of Conduct .
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	-
43	Existence of procedures and mechanisms for exercising the rights of the data subject	-
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	-
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	Yes, see Article 5 of the Ethical Code of Conduct (except international transfers).
46	Provision for right of access for the data subject	Yes, see Article 5 of the Ethical Code of Conduct .
47	Provision for right to rectification	Yes, see Article 5 of the Ethical Code of Conduct .
48	Provision for right to be forgotten and to erasure	-
49	Provision for right to data portability	-
50	Provision for data subject's right to object	Yes, see Article 5 of the Ethical Code of Conduct .
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	-
52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	-
54	Implementing the data security requirements (Article 30)	Yes, see Article 8 of the Ethical Code of Conduct .

55	Notification of a personal data breach to the supervisory authority (Article 31)	-
56	Communication of a personal data breach to the data subject (Article 32)	-
57	Data protection impact assessment (Article 33)	Yes, see Article 8 of the Ethical Code of Conduct .
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	Yes, see Article 8 of the Ethical Code of Conduct .
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	-

11.18 SMART GRID PRIVACY SEAL

	General criteria for evaluation and comparison of privacy seals	Smart Grid Privacy Seal
1	Nature (privacy-oriented/general trust mark)	Privacy seal
2	Country	United States
3	Inception	October 2012. First seal awarded on 28 January 2013.
4	Issuing organisation	The Future of Privacy Forum/TRUSTe
5	Issuer type	Think tank/private company
6	Target of scheme	Companies that use energy data, particularly companies providing services to consumers that rely on energy data
7	Number of certified entities	Currently small; examples given include SDGE Connected, Candi Controls.
8	Renewals	Annual (if equivalent to other TRUSTe programmes).
9	Types of entities that can be certified	<p>Companies offering home energy management, remote home control or security, smart thermostats and other services to consumers seeking to access consumer energy data.</p> <p>The seal does not cover utility collection or use of data for billing, operations, demand response, etc. It also does not apply to companies that are acting as service providers under control of a utility or third party.</p>
10	Type of beneficiaries	<p>Customers, regulators, utilities, companies.</p> <p>According to the website:</p> <ul style="list-style-type: none"> • Consumers: This seal helps to ensure that that a company's practices have been vetted and that consumers will have an avenue for complaint handling and resolution if something goes wrong. • Regulators: Regulators appreciate the additional level of oversight provided by this seal. By participating companies legally commit to responsible practices based on Fair Information Practices informed by the best practices issued by state commissions, NAESB, and NIST. • Utilities: By encouraging third parties to display the seal you help consumers access the information they need to make smart privacy decisions
11	Objective of scheme	<ul style="list-style-type: none"> • Ensure consumer trust in smart devices • Assist utilities in vetting third parties • Allow for a standard consent process to be used across many states

		The seal is not a standard for utilities and does not cover utility collection and use of data for billing, operations, demand response, etc.
12	Descriptive summary of scheme	A dedicated privacy seal scheme for third party companies seeking to use customer energy usage data from smart energy systems to provide customers and utilities with services based upon that data. The scheme is backed and monitored by TRUSTe and appears based on their other privacy seal offerings. The scheme does not cover utility companies and their use of data.
13	Unique selling point	The first seals scheme specifically targeted at smart grid data services
14	Privacy/data protection elements of the scheme	Certificated companies comply with the Future for Privacy Forum's Privacy Guidelines for Smart Grid Guidelines for Customer Energy Data.
15	Guarantees offered to the data subject	None stated.
16	Steps in the certification process	Unclear
17	Coverage of international transfers	Not stated.
18	Costs (i.e., evaluation cost, certification cost)	Not stated.
19	Validity	Not stated.
20	Revocation mechanism	Not stated.
21	Recognition	<p>To create the program, the Future of Privacy Forum and TRUSTe worked with companies including AT&T, Comcast, Ecofactor, IBM, Intel, Motorola, Neustar, Opower, Tendril, and Verizon. Utilities and utility regulators provided input on the program.</p> <p>The Future of Privacy Forum is a Washington, DC based think tank supported by industry</p>
22	Accredited experts and/or evaluation bodies	The program anticipates an advisory committee including the Edison Electric Institute, the GridWise Alliance and consumer advocates.
23	Duration and scope of the certification process	Not stated.
24	Number of certified experts and/or bodies	Not stated.
25	Regulatory/ compliance standards	<p>Certification ensures that companies are in accord with the Future for Privacy Forum's Smart Grid Privacy Guidelines and TRUSTe's program requirements for Smart Grid.</p> <p>The FPF privacy guidelines were developed with reference to the FTC's Fair Information Practice Principles, the OECD Privacy guidelines, privacy by design, North American Energy Standards Board recommended standards for Third-Party Access to Smart Meter-based information and California Public Utilities Commission rules</p>

		regarding privacy and security.
26	Frequency and means of updates to scheme	Not stated
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	Not stated.
28	Complaints mechanism	<p>The website states: You may report violations of a participant’s posted privacy statement and specific privacy issues with a participant’s smart device/service. TRUSTe investigates all eligible complaints and mediates solutions. Before you submit a complaint to TRUSTe, you should attempt to contact the site you are reporting directly to allow them to resolve your concern. Complaints to smartgrid-feedback@questions.truste.com and must include the following information:</p> <ul style="list-style-type: none"> • Your name • Name of service provider • Website address or application name • Description of your issue • Description of requested resolution • Date that you reported your concern to the provide • The provider’s response to your complaint.
29	Criticisms	<ul style="list-style-type: none"> • The TRUSTe Program Requirements were missing from the TRUSTe website, with incorrect links. • The scheme does not cover the use of anonymised data that cannot identify an individual or an individual’s household.
30	Links and references to the scheme	<ul style="list-style-type: none"> • Future of Privacy Forum, “Smart Grid Privacy Guidelines for Customer Energy Data”. http://www.futureofprivacy.org/wp-content/uploads/FPF_Smart_Grid_Guidelines.pdf • TRUSTe, “Smart Grid program requirements”. - http://www.truste.com/privacy-program-requirements/home • Carson, Angelique, “Stakeholders Aim To Craft Smart Grid Privacy Code of Conduct” 27 Feb 2013. https://www.privacyassociation.org/publications/2013_02_27_stakeholders_aim_to_craft_smart_grid_privacy_code_of_conduct
31	Logo	
32	Website	http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-smart-grid
	General data protection regulation requirements under Ch II and III	


33	Fair, lawful, transparent processing of personal data	
34	Data collection for specified, explicit and legitimate purposes	The Smart Grid Privacy Guidelines state: Covered Companies relying on customer energy use data should in their notifications clearly and plainly articulate the purpose and use of the data that they will collect. When Covered Companies adopt additional uses of previously collected customer energy use data and those additional uses are materially different from uses that had previously been disclosed and authorized, Companies shall notify consumers of such changes and obtain their affirmative consent to the change.
35	Adequate, relevant and limited data collection	Not stated.
36	Data accuracy	Not stated.
37	Time and purpose restricted data retention	The Smart Grid Privacy Guidelines state: Covered Companies should collect and retain only the customer energy use data for which they have specific business purposes. Covered Companies should establish policies regarding the retention of collected data and delete or otherwise securely dispose of the collected data when they no longer have a specific and legitimate present or anticipated business purpose. Covered Companies should also ensure by contract that their partners' or agents' data retention and minimization policies provide equivalent or greater protections.
38	Data is processed under the responsibility and liability of the controller	The Smart Grid Privacy Guidelines state: customer energy use data sent to third parties that does not need to be used or maintained in personally identifiable form should be aggregated and/or anonymized before being transmitted to third parties.
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not stated.
40	Consent requirement for processing of special personal data	The Smart Grid Privacy Guidelines state: Covered Companies relying on customer energy use data should seek consent for the collection, storage, use, and disclosure of that information. Covered Companies should tailor the type of consent to the nature of the specific data collected and its intended use, including how it will be shared with others. Initial affirmative consent is required to collect or share energy use data that contains personally identifying information, but may be implied for commonly accepted uses or sharing by a covered Company when a consumer has been afforded the notification required above and provides customer energy use data to obtain a service. Affirmative consent is also required when a Covered Company adopts additional uses of previously collected customer energy use data containing PII and the changes would likely affect the consumer's decisions about the service if she were to be

		<p>informed of them. Where affirmative consent is necessary, the particular notice and consent mechanism used should be appropriate to the particular situation and could encompass a range of options, including consumer profile management, click-through, check box, telephone, keypress, traditional signature or other mechanisms.</p> <p>Consumers who decline to accept a material change in the use of their information may have to forgo service or receive a different tier of service.</p>
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	<p>The Smart Grid Privacy Guidelines state: Covered Companies should notify consumers in a clear and transparent manner about their data management practices regarding the collection, storage, use, and disclosure of customer energy use data where the data consists of personally identifiable information (PII), which is data that can be reasonably linked to a specific individual or household.</p> <p>In addition to any real-time or other enhanced notices, Covered Companies should ensure their privacy policies are accessible and reasonably comprehensible to the intended audience. The privacy policies should be concise and include descriptions of the types of data that will be used, how the data will be used, and any options consumers have for controlling such use.</p>
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	<p>The Smart Grid Privacy Guidelines state: Covered Companies should notify consumers in a clear and transparent manner about their data management practices regarding the collection, storage, use, and disclosure of customer energy use data where the data consists of personally identifiable information (PII), which is data that can be reasonably linked to a specific individual or household.</p>
43	Existence of procedures and mechanisms for exercising the rights of the data subject	<p>The Smart Grid Privacy Guidelines state: Covered Companies will use best efforts to address and resolve any issues or problems raised by consumers relating to PII.</p>
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not stated.
45	<p>Provision of information to data subject:</p> <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation on the level of protection afforded by that third country 	<p>The Smart Grid Privacy Guidelines state: Covered Companies shall develop internal mechanisms to respond to any consumer inquiries regarding PII and shall provide contact information where consumers can submit their concerns to the Covered Company.</p>

	international organisation by reference to an adequacy decision by the Commission <ul style="list-style-type: none"> Any further information necessary to guarantee fair processing 	
46	Provision for right of access for the data subject	The Smart Grid Privacy Guidelines state: Upon request, Covered Companies should - to the extent reasonably feasible and proportionate to the sensitivity of the data involved - provide consumers convenient and secure access to customer energy use data.
47	Provision for right to rectification	Not stated.
48	Provision for right to be forgotten and to erasure	Not stated.
49	Provision for right to data portability	Not stated.
50	Provision for data subject's right to object	Not stated, but consent is flagged as an important basis for companies using customer energy data.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not stated.
52	Rights in relation to automated processing	Not stated.
53	Documentation requirements (Art 28)	Not stated.
54	Implementing the data security requirements (Article 30)	The Smart Grid Privacy Guidelines state: Covered Companies relying on customer energy use data to offer functionality for their products should implement reasonable administrative, technical, and physical safeguards to protect the data from unauthorized access.
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not stated.
56	Communication of a personal data breach to the data subject (Article 32)	The Smart Grid Privacy Guidelines state: In the event of a breach of customer energy use data covered by applicable data breach notification laws, Covered Companies should notify potentially affected individuals within the timeframes set in the applicable law(s).
57	Data protection impact assessment (Article 33)	The Smart Grid Privacy Guidelines state: Covered Companies should achieve such security and data quality standards by proactively anticipating and mitigating the risk of potentially invasive events and designing their products accordingly.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not stated.
59	Designation of a data protection officer (Article 35(1))	Not stated.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	The Smart Grid Privacy Guidelines state: Covered Companies should participate in self-regulatory programs administered by third parties where available, which shall have dispute resolution processes to address disputes not addressed at the Covered Company.

11.19 TRANSACTION GUARD PRIVACY POLICY VERIFIED SEAL

	General criteria for evaluation and comparison of privacy seals	TransactionGuard Privacy Policy Verified Seal
1	Nature (privacy-oriented/general trust mark)	Privacy mark
2	Country	USA
3	Inception	-
4	Issuing organisation	Transaction Guard LLC
5	Issuer type	Limited Liability Company
6	Target of scheme	Internet sellers
7	Number of certified entities	Data not found.
8	Renewals	Data not found.
9	Types of entities that can be certified	Private organisations
10	Type of beneficiaries	Internet consumers
11	Objective of scheme	To show prospective website customers that a business's privacy practices have been thoroughly examined and that their personal information is 100% secure.
12	Descriptive summary of scheme	According to Transaction Guard , the Transaction Guard Privacy Policy and Privacy Seal are additions to a website that serve to satisfy its customers' need for privacy and security. Transaction Guard online security experts design a privacy policy for the respective website while thoroughly evaluating and examining its privacy practices to confirm their validity and professionalism, to suggest changes and improvements, to confirm why it needs the information it collects, how it is going to be used it and how it is going to be kept private and safe.
13	Unique selling point	Transaction Guard online security experts draft a privacy policy for websites undergoing the certification process. The policy is intended to be " 100% compliant with all the major search engines such as Google, Yahoo, MSN, etc. "
14	Privacy/data protection elements of the scheme	Information is not available (no code or standards against which evaluation and certification takes place are available online).
15	Guarantees offered to the data subject	Safety of personally identifiable information.
16	Steps in the certification process	-
17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification cost)	\$9.95 per month or \$97.00 per year
19	Validity	-
20	Revocation mechanism	-

21	Recognition	-
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	-
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	The Privacy Policy to be drafted is intended to be “ 100% compliant with all the major search engines such as Google, Yahoo, MSN, etc. ”
26	Frequency and means of updates to scheme	-
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	-
28	Complaints mechanism	-
29	Criticisms	<ul style="list-style-type: none"> • No certification policy or standards are available on the website. • A mixed role of certification and privacy policy creator, undertaking both certification task and the task of drafting a (compliant) privacy policy.
30	Links and references to the scheme	-
31	Logo	
32	Website	http://www.transactionguard.com
	General data protection regulation requirements under Ch II and III	GDPR-related analysis was not possible due to non-availability of scheme criteria and requirements.
33	Fair, lawful, transparent processing of personal data	-
34	Data collection for specified, explicit and legitimate purposes	-
35	Adequate, relevant and limited data collection	-
36	Data accuracy	-
37	Time and purpose restricted data retention	-
38	Data is processed under the responsibility and liability of the controller	-
39	Provision for parental consent based processing of personal	-


	data of a child below the age of 13	
40	Consent requirement for processing of special personal data	-
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	-
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	-
43	Existence of procedures and mechanisms for exercising the rights of the data subject	-
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	-
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country, international organisation and level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	-
46	Provision for right of access for the data subject	-
47	Provision for right to rectification	-
48	Provision for right to be forgotten and to erasure	-

49	Provision for right to data portability	-
50	Provision for data subject's right to object	-
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	-
52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	-
54	Implementing the data security requirements (Article 30)	-
55	Notification of a personal data breach to the supervisory authority (Article 31)	-
56	Communication of a personal data breach to the data subject (Article 32)	-
57	Data protection impact assessment (Article 33)	-
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	-
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	-

11.20 TRUSTE

	General criteria for evaluation and comparison of privacy seals	TRUSTe
1	Nature (privacy-oriented/general trust mark)	Website privacy seal.
2	Country	USA
3	Inception	1997
4	Issuing organisation	TRUSTe
5	Issuer type	Online privacy solutions provider, incorporated in 2008.
6	Target of scheme	Online companies and organisations.
7	Number of certified entities	According to its website , TRUSTe has over 5,000 clients including Apple, Disney, eBay, Forbes, HP, and Microsoft.
8	Renewals	Annual
9	Types of entities that can be certified	Online companies and organisations.
10	Type of beneficiaries	Online consumers, public.
11	Objective of scheme	TRUSTe's website suggests that the objective of the scheme is to "signal to consumers that a website is safeguarding your personal information and values your online privacy".
12	Descriptive summary of scheme	The TRUSTe web privacy seal certifies that companies adhere to TRUSTe's privacy requirements.
13	Unique selling point	<ul style="list-style-type: none"> • Most widely and universally recognised privacy seal. • Free online privacy dispute resolution.
14	Privacy/data protection elements of the scheme	Use of personally identifiable information (PII) and third party PII, choice, online directory opt-outs, data quality, access and security.
15	Guarantees offered to the data subject	<ul style="list-style-type: none"> • Responsible use of PII • Choice • Opt-out • Data quality • Access • Security
16	Steps in the certification process	<ol style="list-style-type: none"> 1. Participant completes a formal application to become a TRUSTe participant. 2. TRUSTe independently reviews the participant's privacy statement and self-assessment. 3. Grant of certification mark.
17	Coverage of international transfers	-
18	Costs (i.e., evaluation cost, certification cost)	Annual fee based on applicant's annual revenue.

19	Validity	One year (annual re-certification).
20	Revocation mechanism	<p>Upon material breach of its Program Requirements, TRUSTe may revoke/terminate a participant's participation in its privacy program with 20 business days' prior written notice unless the breach is corrected within the same period. Material breaches include but are not limited to:</p> <ul style="list-style-type: none"> • Participant's continual, intentional, and material failure to adhere to Program Requirements. • Participant's material failure to permit or cooperate with a TRUSTe investigation or review of its online properties or practices. • Participant's continual, intentional, and material failure to comply with any suspension obligations. • Participant's material failure to cooperate with TRUSTe regarding an audit, complaint or the compliance monitoring activities of TRUSTe. • Any deceptive trade practices.
21	Recognition	According to a TRUSTe 2010 Brand Awareness Study , 40% of the top fifty most trafficked websites display the TRUSTe seal, more than 20 twenty million consumers click the TRUSTe seal annually to verify a site's certification and 82% of consumers trust TRUSTe and find the privacy trust mark useful in deciding when and how to disclose personal information.
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	<p>Variable.</p> <p>Scope: As defined in the TRUSTe Privacy Program Requirements.</p>
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	TRUSTe Privacy Program Requirements .
26	Frequency and means of updates to scheme	Not clear.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	Additional email requirements, mobile services requirements. Coverage of social networks.
28	Complaints mechanism	Complainant must first confirm the website is a TRUSTe client, verify that the complaint is a privacy matter relating to a TRUSTe client website, and contact the TRUSTe client website. If the TRUSTe client does not resolve the complaint, the complainant can use the TRUSTe Dispute Resolution Program (complete an online dispute resolution form). The process is free.
29	Criticisms	- The TRUSTe seal has been illegally displayed in

		<p>the past.</p> <ul style="list-style-type: none"> - Ineffective oversight of member organisations. - Over-reliance on applicants claims.
30	Links and references to the scheme	<ul style="list-style-type: none"> - Edelman, Benjamin, “Coupons.com and TRUSTe: Lots of Talk, Too Little Action”, 18 March 2008. http://www.benedelman.org/news/031808-1.html - Stark, David and C. Hodge, “Consumer behaviors and attitudes about privacy: A TNS/TRUSTe study”, TNS/ TRUSTe, 2004, http://www.truste.org/pdf/Q4_2004_Consumer_Privacy_Study.pdf - Benassi, Paola, “TRUSTe: An online privacy program”, <i>Communications of the ACM</i>, Vol. 42, No. 2, 1999, pp. 56-59.
31	Logo	
32	Website	http://www.truste.com/
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	The <i>Use of PII</i> principle of the TRUSTe Privacy Program Requirements prescribes that a participant must use PII providing advertised services in accordance with its posted privacy statement in effect at the time of collection, or with notice and consent as described in the Program Requirements. However, information collected by the participant or the participant’s service provider may be used to tailor an individual’s experience on the relevant website.
34	Data collection for specified, explicit and legitimate purposes	The <i>Collection Limitation</i> principle of the TRUSTe Privacy Program Requirements prescribes that PII shall only be collected where such collection is either limited to information reasonably useful for the purpose for which it was collected and in accordance with the participant’s privacy statement at the time of collection, or with notice to and consent of the individual.
35	Adequate, relevant and limited data collection	As above.
36	Data accuracy	The <i>Data Quality</i> principle of the TRUSTe Privacy Program Requirements prescribes that a participant must take commercially reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PII to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used.
37	Time and purpose restricted data retention	The TRUSTe Privacy Program Requirements prescribe: If a participant receives and retains PII or third party PII, it must limit PII retention to no longer than commercially useful, to carry out its business purpose, or legally required; and must disclose in its privacy statement for how long it will retain that information.

		Regardless of the time period of retention, so long as PII or third party PII is retained in possession or control, the requirements apply to such information
38	Data is processed under the responsibility and liability of the controller	-
39	Provision for parental consent based processing of personal data of a child below the age of 13	In relation to social networks, the TRUSTe Privacy Program Requirements provide that individuals between the ages 13-17 must provide express consent to the collection, use, disclosure of their PII or third party PII pertaining to individuals between the ages of 13-17.
40	Consent requirement for processing of special personal data	Express consent is required for processing PII of individuals between ages of 13-17.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Access to the privacy statement shall be clear and conspicuous. As commercially reasonable, the privacy statement must be available when the individual engages with the participant, such as through an application, website, homepage or landing page.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	The participant must maintain and abide by an accurate up-to-date privacy statement (approved by TRUSTe in its sole discretion) that outlines the participant's information practices and is in conformance with the TRUSTe Privacy Program Requirements .
43	Existence of procedures and mechanisms for exercising the rights of the data subject	<p>The TRUSTe Privacy Program Requirements prescribe that participants must implement reasonable and appropriate mechanisms to allow individuals to correct or update inaccurate PII. Instructions or links to a mechanism that enables individuals to withdraw consent for the use of their information for the purposes of behavioural advertising must be provided.</p> <p>In relation to social networks, the TRUSTe Privacy Program Requirements prescribe that a reasonable and appropriate mechanism must be provided to allow individuals to manage their privacy settings. Participants must provide a reasonable and appropriate mechanism to allow individuals to request deletion or deactivation of profiles and a reasonable and appropriate mechanism to request removal of unauthorised profiles. The mechanism should be consistent with how the individual normally interacts or communicates with the participant.</p>
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	The TRUSTe Privacy Program Requirements prescribe that a participant shall confirm that individual inaccuracies have been corrected.
45	Provision of information to data subject: <ul style="list-style-type: none"> identity and the contact details of controller 	A participant's privacy statement must include (but not limited to): information collected actively or passively and how it is used; types of third parties with whom information is shared; whether PII is appended with

	<ul style="list-style-type: none"> • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipient personal data • Transfer to a third country or international organisation and of level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	<p>information obtained from third party sources; how and when the individual can exercise choice; how the individual can request access to their information; the types of security measures in place to protect collected information; the tracking technologies used; how the individual can contact the participant, including company name, email address or a link to an online form, and physical address; how the individual will be notified of any material changes in the participant's privacy practices; what collected information is subject to disclosure pursuant to judicial or other government subpoenas, warrants, orders, or if the participant merges with or is acquired by a third party, or goes bankrupt; the effective date of privacy statement; statement of participation in the TRUSTe program and participation scope; and information on how to contact TRUSTe to express concerns regarding participant's privacy statement or privacy practices.</p>
46	Provision for right of access for the data subject	<p>The principle of <i>Access</i> in the TRUSTe Privacy Program Requirements provides that a</p> <ol style="list-style-type: none"> Participant must implement reasonable and appropriate mechanisms to allow the individual to correct or update inaccurate PII. Participant must implement reasonable mechanisms to allow the individual to request deletion of PII or that collected PII no longer be used. Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant Such mechanism or process shall be clear, conspicuous, and easy to use Such mechanism or process shall confirm to the individual inaccuracies have been corrected; and Participant's privacy statement shall state how access is provided.
47	Provision for right to rectification	The participant must implement reasonable and appropriate mechanisms to allow individuals to correct or update inaccurate PII.
48	Provision for right to be forgotten and to erasure	The participant must implement reasonable mechanisms to allow individuals to request deletion of PII or that collected PII no longer be used.
49	Provision for right to data portability	-
50	Provision for data subject's right to object	Participant must provide individuals with an opportunity to withdraw consent to the use of PII for secondary purposes. The participant must provide the individual with a <i>Just in Time Notice</i> and the opportunity to withdraw consent to having PII disclosed or distributed to third parties other than service providers, at the time PII is collected. The participant must provide a means by which the individual can change their choice selection.

51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Prior to sending commercial or promotional email messages, targeted recipients must have an opportunity to withdraw consent to having their email addresses added to a mailing list. Commercial or promotional email messages sent under this form of consent must include a 'clear and conspicuous identification' that the message is an advertisement or solicitation.
52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	-
54	Implementing the data security requirements (Article 30)	<p>The <i>Data Security</i> principle of the TRUSTe Privacy Program Requirements prescribes:</p> <p>a. Participant must implement commercially reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution.</p> <p>b. Participant shall maintain and audit internal information technology systems within participant's control such as:</p> <ul style="list-style-type: none"> -Regularly monitor and repair systems including servers and desktops for known vulnerabilities; -Limit access and use of PII, or third party PII, to personnel with a legitimate business need where inappropriate access, use, or disclosure of such PII, or third party PII, could cause financial, physical, or reputational harm to the individual; - Implement protection against phishing, spam, viruses, data loss, and malware; and - Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual <p>c. Participant shall utilise encryption such as Secure Socket Layer for the transmission of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.</p> <p>d. Access to PII or third party PII retained by Participant must be at least restricted by username and password if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.</p> <p>e. Privacy Statement shall state that security measures are in place to protect collected PII and/or third party PII.</p>
55	Notification of a personal data breach to the supervisory authority (Article 31)	A participant must notify TRUSTe when it believes a data breach has occurred and provide TRUSTe with a copy of the notice sent (or to be sent) to affected individuals.
56	Communication of a personal data breach to the data subject	A participant must notify an individual of a data breach within 45 days of a known breach as required by law or


	(Article 32)	if the unauthorized disclosure of PII can cause financial, physical, or reputational harm to the individual unless otherwise required by law.
57	Data protection impact assessment (Article 33)	-
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	-
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	A participant must maintain and audit internal information technology systems within participant's control.

11.21 TRUSTED SHOPS

	General criteria for evaluation and comparison of privacy seals	Trusted Shops
1	Nature (privacy-oriented/general trust mark)	European trust mark
2	Country	Germany
3	Inception	Trusted Shops was founded in 1999.
4	Issuing organisation	Trusted Shops
5	Issuer type	Private commercial organisation
6	Target of scheme	Online shops
7	Number of certified entities	15,046 certified shops (according to website)
8	Renewals	-
9	Types of entities that can be certified	In principle, all online shops that offer their customers a fully web-based ordering process with a shopping basket system can be certified by Trusted Shops. However, the following are excluded: <ul style="list-style-type: none"> • Shops that sell product groups/products listed in the Trusted Shops exclusion catalogue. • Pure portals without sales activities.
10	Type of beneficiaries	Online consumers
11	Objective of scheme	To guarantee the safety of online shopping and security of consumers. To help consumers shop online with peace of mind. To offer reliable buyer protection.
12	Descriptive summary of scheme	Online retailers are subjected to comprehensive security tests. This testing, with over 60 individual criteria, is based on consumer protection requirements as well as national and European legislation. These include creditworthiness, security mechanisms, price transparency, provision of information, customer service and data protection. These quality criteria are subjected to constant review and adapted to the latest developments in the areas of case law and consumer protection.
13	Unique selling point	Shops awarded the Trusted Shops Seal of Approval offer consumers Buyer Protection.
14	Privacy/data protection elements of the scheme	<ul style="list-style-type: none"> - Calls for compliance with applicable data protection law - Privacy policy - Consent for data collection, processing and use - Technical and organisational measures.
15	Guarantees offered to the data subject	<ul style="list-style-type: none"> - Appropriate security measures must be used to protect customers' personal and other data. - The customer must be informed in the Privacy Policy about the right to revoke their consent at any time in the future.

		<ul style="list-style-type: none"> - Transparency in the retailer's use of personal information. - Compliance with EU data protection legislation
16	Steps in the certification process	<ol style="list-style-type: none"> 1. Preparation (approximately 1-2 weeks) 2. Auditing and subsequent correction (approximately 2 weeks) 3. Final acceptance after retailer reports back 4. Integrating the technology (integration of the page enabling registration for buyer protection and the Trusted Shops Seal of Approval in the retailer's shop after final acceptance has been approved) 5. Trusted Shops activates retailer's shop by setting the certification status to 'VALID' following certification and advertise the shop, among others, on the Trusted Shops portal.
17	Coverage of international transfers	Covered as part of EU legal requirements.
18	Costs (i.e., evaluation cost, certification cost)	<p>The monthly membership fee includes a standing charge (based on gross online annual revenues of members and ranges between £10-319 and which is reduced when pre-certified shop software is used) and a monthly certificate fee of £29 for each registered certificate. There are optional extra packages and further membership costs such as a one-off set-up fee (£79), processing fee (£25 per claim), cost of additional audit report in case of insufficient implementation of the first audit report (£50). Costs of Buyer Protection service (Excellence Integration) range from £0.98 - £39.20 per 30 days.</p> <p>Additional services cost as follows:</p> <ul style="list-style-type: none"> - Express audit accelerated audit of all quality criteria in maximum three work days (subject to appraisal of creditworthiness) - £200 - Change of shop ownership assignment and acceptance of existing contract (shop is untouched, e.g. terms and conditions etc.) - £90 - Change of shop solution re-audit due to change of shop solution -£200 - Re-audit due to significant modifications to the online shop with regard to the Trusted Shops quality criteria - £200 - Certificate for additional shop additional audit report, certificate and shop profile with logo, description and link - £29 per month
19	Validity	<p>General Membership Conditions: The trust mark usage rights are only granted after a successful initial audit of the online shop by Trusted Shops, for the duration of the term of the contract, provided that the online shop fulfils the conditions of use.</p>

20	Revocation mechanism	<p>General Membership Conditions: The trust mark usage right shall be forfeited as soon as and as long as the online shop fails to fulfil one or more of the above requirements. Trusted Shops shall inform the online shop of this infringement and grant the latter a reasonable time limit to comply with the conditions of use. If the conditions of use are not fulfilled after the time limit has expired, Trusted Shops will be able to set the status of the seal to 'blocked', so that customers of the online shop are no longer able to register for the Trusted Shops Guarantee.</p> <p>Trusted Shops shall again audit the online shop after blocking the seal at its own discretion, to determine whether it is complying with the conditions of use. If the online shop has eliminated all the violations of the conditions of use, Trusted Shops will switch the status of the seal from 'blocked' to 'valid'. All costs which arise as a result of Trusted Shops having to audit the online shop again in connection with violations of the conditions of use will be borne by the online shop according to the agreed Price List.</p>
21	Recognition	<p>According to itself, Trusted Shops is supported by the European Commission for its effective consumer protection and the promotion of SMEs and recommended by the D21 initiative.</p> <p>Trusted Shops is business partner of the European E-commerce and Mail Order Trade Association (EMOTA), a consortium of European shipping trade associations.</p>
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	<p>The retailer generally receives the audit report for the shop within 3-4 weeks of acceptance of the order by Trusted Shops.</p> <p>See Item 16 (steps in the certification process)</p>
24	Number of certified experts and/or bodies	-
25	Regulatory/ compliance standards	<p>The quality criteria for the respective target markets is listed country wise: Germany, France, Austria, Poland, Switzerland, Spain, United Kingdom and Other EU country. These quality criteria are based on consumer protection requirements as well as national and European legislation. Also applicable are the Trusted Shops General Membership Conditions and the ISIS/TS Code of Practice.</p>
26	Frequency and means of updates to scheme	Not clear.

27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	Links to consumer protection.
28	Complaints mechanism	<p><u>General Membership Conditions</u>: For the term of the contract the online shop must respond within five business days to enquiries submitted by Trusted Shops and customers - at the sole discretion of Trusted Shops - either via the online system provided to the online shop by Trusted Shops, or by email or in writing in an appropriate form and submit all the documents necessary for processing within that period, irrespective of whether or not the customer in the case at issue has registered for the Trusted Shops Guarantee.</p> <p>If, in spite of having been issued with a demand and after the expiry of the grace period, the online shop culpably breaches these cooperation obligations, Trusted Shops may claim a processing fee in accordance with its price list for each case of damage or complaint. The online shop shall be at liberty to provide proof that no damage occurred or that the resulting entitlement to compensation is lower than the flat amount.</p>
29	Criticisms	Existence of procedures and mechanisms for exercising the rights of the data subject could be more easily and accessibly presented.
30	Links and references to the scheme	<ul style="list-style-type: none"> - Grabner-Kraeuter, Sonja, "The role of consumers' trust in online-shopping", <i>Journal of Business Ethics</i>, Vol. 39, Iss. 1-2, 2002, pp. 43-50. - Winkelmann, Axel, Matthias Boehm, and Jörg Becker, "Usability of "Trusted Shops: An Empirical Analysis of eCommerce Shops, <i>SIGHCI 2008 Proceedings</i>, Paper 8. http://aisel.aisnet.org/sighci2008/8
31	Logo	 <p>TRUSTED SHOPS® The trustmark with buyer protection</p>
32	Website	http://www.trustedshops.com/
General data protection regulation requirements under Ch II and III		
33	Fair, lawful, transparent processing of personal data	<p><u>The ISIS/TS Code of Practice</u> Required criteria: Merchants, and others responsible for administering e-commerce services must ensure that the way they compile and use personal information about consumers conforms to the EU data protection legislation. The merchant must ensure at all times that their practice regarding the use of personal information is in accordance with applicable data</p>

		protection law.
34	Data collection for specified, explicit and legitimate purposes	The ISIS/TS Code of Practice Required criteria: The merchant must ensure at all times that their practice regarding the use of personal information is in accordance with applicable data protection laws.
35	Adequate, relevant and limited data collection	The ISIS/TS Code of Practice Required criteria: the merchant must ensure that personal data are only held for as long as needed and for the purpose it was collected.
36	Data accuracy	The ISIS/TS Code of Practice Required criteria: The merchant must ensure that personal data are accurate and up to date.
37	Time and purpose restricted data retention	The ISIS/TS Code of Practice Required criteria: Customer personal information should be kept no longer than is necessary.
38	Data is processed under the responsibility and liability of the controller	Implicit.
39	Provision for parental consent based processing of personal data of a child below the age of 13	The ISIS/TS Code of Practice Required criteria: In particular, the law relating to obtaining such information from minors (i.e. a person under 18 years of age) should be strictly adhered to and best practice (for ex-ample compliance with the Direct Marketing Association Code of Practice) implemented - no information about a child under 12 years of age may be collected without the explicit verifiable consent of his/her parent or guardian, and no information about a child under the age of 14 may be disclosed to anyone else without the consent of their parent or guardian.
40	Consent requirement for processing of special personal data	Not explicitly mentioned, but would apply by virtue of: The ISIS/TS Code of Practice Required criteria: The merchant must ensure at all times that their practice regarding the use of personal information is in accordance with applicable data protection laws.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	The ISIS/TS Code of Practice Audit criteria: Merchants are strongly encouraged to publish their Privacy Policy concerning the merchant's use of customer personal information, which policy should conform to any applicable codes or practice or guidance published by the UK Information Commissioner.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	The Trusted Shops Quality criteria provide All information provided on the supplier's website must be provided in a clear, intelligible, easily accessible and unambiguous manner.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	The ISIS/TS Code of Practice Audit criteria: The merchant is required to notify the customer in advance of an order being placed how communication will be facilitated (e-mail and/or telephone facilities will be the minimum, and a valid email address must be provided at all times), its


		timeliness (how quickly responses will be made), how to correct input errors, the availability of services (e.g. office hours, public holidays) and provide all requisite contractual information in a designated language(s).
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	-
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	<p>The Trusted Shops Quality criteria provide: The supplier must provide in a clear and comprehensible manner certain information identifying the supplier in a ‘supplier identification’ section on the web-site. It must be prominent, easily, directly and permanently accessible in characters that can be read with the naked eye. Supplier identification must include the following details: the name and legal status of the supplier; the geographical address at which the service provider is established (street, postcode, location); contact details (including e-mail address and phone number) for customer enquiries (i.e. customer service information); if the supplier is a company or other corporate body, its registered office, the part of the UK in which the company is registered and its company registration number; if applicable, the supplier’s VAT number; if applicable, the details of any professional body or similar institution with which the supplier is registered, the professional title and the Member State where that title has been granted as well as a reference to the professional rules applicable to the supplier; details of any relevant supervisory scheme relating to the provision of the service.</p> <p>The ISIS/TS Code of Practice Audit criteria: the merchant must ensure at all times that their practice regarding the use of personal information is transparent to the customer (i.e. the consumer should be told what data is being collected, how, by whom, what for, and of their right to have such data kept up to date). Merchants should provide information relating to their use of cookies on their websites. This includes the storage of data specific to an individual's use on the customer's own computer.</p>
46	Provision for right of access for the data subject	-
47	Provision for right to rectification	-
48	Provision for right to be forgotten and to erasure	-
49	Provision for right to data portability	-
50	Provision for data subject’s right to object	The ISIS/TS Code of Practice Audit criteria: The customer must be informed in the Privacy Policy about the right to revoke their consent at any time in

		the future
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	The ISIS/TS Code of Practice Best practice: If the merchant proposes to provide personal information about a customer to third parties, or use such data itself, for direct marketing purposes, ISIS/TS recommends that the customer should be given the option to opt-in as opposed to the option to opt-out (although 'opt-out' may in certain circumstances be acceptable). The customer would therefore specifically consent to the inclusion of their information in such a provision.
52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	-
54	Implementing the data security requirements (Article 30)	The ISIS/TS Code of Practice Required criteria: Appropriate security measures must be used to protect customers' private information, order details, credit card numbers and banking information in storage. The ISIS/TS Code of Practice Audit criteria: Appropriate security measures must be used to protect customers' private information, order details, credit card numbers and banking information, during transmission.
55	Notification of a personal data breach to the supervisory authority (Article 31)	-
56	Communication of a personal data breach to the data subject (Article 32)	-
57	Data protection impact assessment (Article 33)	-
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	-
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	General Membership Conditions : After a period of 12 months, Trusted Shops shall audit the online shop again, at its own discretion either completely or partially, to ensure it is complying with the conditions of use (follow-up audit). Trusted Shops is entitled at its sole discretion and at irregular intervals to check in its own right or commission authorised third parties to check for compliance with the terms and conditions of use (§ 2.5) (extraordinary audit).

11.22 TRUSTIFY-ME PRIVACY CERTIFICATION SEAL

	General criteria for evaluation and comparison of privacy seals	Trustify-me Privacy Certification Seal
1	Nature (privacy-oriented/general trust mark)	Privacy seal
2	Country	According to its website, “Trustify-me offers services in many countries across the globe but mostly English speaking countries including the US, Canada, UK, New Zealand, Australia, etc.”
3	Inception	Website launched 2006
4	Issuing organisation	Trustify-me.org (occasionally referred to as ‘Trust Seal’ in documentation).
5	Issuer type	Trustify-Me appears to be a private company (no information about legal constitution appears on the website, has .org address, the domain is registered by domainsbyproxy.com).
6	Target of scheme	Websites.
7	Number of certified entities	Not stated. Small number of entities returned from a Google search; several of these had the same registered address.
8	Renewals	Monthly or yearly, discounts available for commitment of more than a year. No information given on how often websites are recertified.
9	Types of entities that can be certified	Websites. Trustify-me does not verify websites in languages other than English or not having an English option.
10	Type of beneficiaries	Commerce websites, website users and visitors.
11	Objective of scheme	To assure customers and increase the likelihood that customers will buy from websites carrying the seal.
12	Descriptive summary of scheme	<p>The Privacy Certification seal is one of four Trustify-me seals (including security certification seal, business certification seal and personal certification seal). Websites pay a monthly or yearly fee to display a customised privacy seal on their website (the seal contains the name of the website, and the date of certification) following an assessment of the website’s privacy policy.</p> <p>Clicking on seal on a member website links back to a page at trustify-me.org which provides contact details and address for the website, as well as the date of certification.</p>
13	Unique selling point	Custom seal, allow addition of domain name to the Trustify-me seals. Lower price. Additionally, A date should be present on most Trustify-me seals to inform visitors that the seal and service are current and that the website is in good standing with the issuer of the seal.
14	Privacy/data protection elements of the scheme	Privacy policy verification.

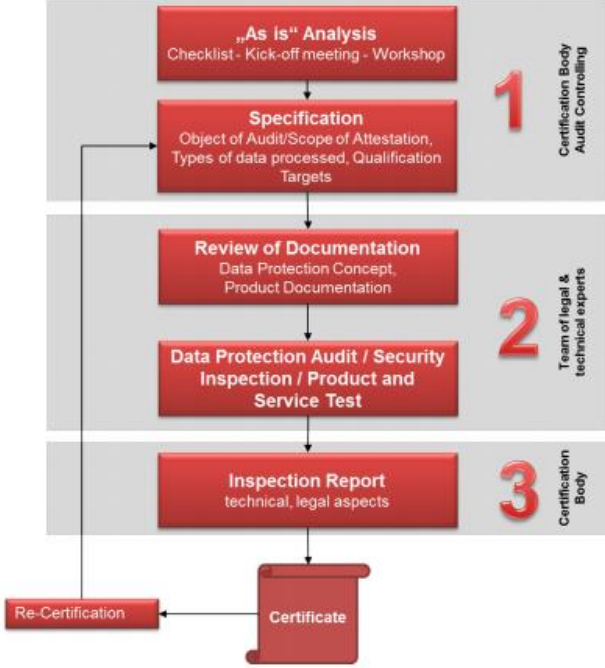
15	Guarantees offered to the data subject	<p>Offers third party privacy resolution services to anyone that feels that their privacy rights may be in question. No detail on how this occurs or is achieved.</p> <p>Trustify-me states it “shall not be liable for any special or consequential damages that result from the use of, or the failure to use, the services and products offered on this site, or the performance of the services and products. Trustify-me is a verification service, and as such, attempts to verify the information that Trustify-me receives using logical means. Trustify-me does not guarantee or warranty any information that they gather or use.”</p>
16	Steps in the certification process	<p>Trustify-me reviews customers privacy policies to see that they directly address third party disclosure, private information security measures and email notifications. No on-site audit or active testing.</p> <p>Trustify-me conveys that (for a typical website), it verifies: support email, phone, business address, seal header, privacy policy and SSL certificate expiration. Trustify-me also requires its customers to provide it with the following information for a Trustify-me Privacy Verification: website URL, business address, phone number, e-mail address and privacy policy.</p>
17	Coverage of international transfers	Not stated
18	Costs (i.e., evaluation cost, certification cost)	\$19 per month, \$197 per year. Discounts if the privacy seal purchased as part of a bundle with business and security seals, or if signing up for several years.
19	Validity	Immediately following certification process. Monthly or yearly validity.
20	Revocation mechanism	Trustify-me’s Terms of Use state, “Due to the nature of the services provided, Trustify-me reserves the right to take out seals from any website and/or cancel any account for any reason at their judgment without prior notice or announcement.”
21	Recognition	Trustify-me seals are included as part of e-buy360.com e-commerce package. See http://e-buy360.com/
22	Accredited experts and/or evaluation bodies	None stated.
23	Duration and scope of the certification process	Not stated, appears short and of minimal scope.
24	Number of certified experts and/or bodies	Not stated.
25	Regulatory/ compliance standards	No specific regulatory or compliance standards are stated. Trustify-me only suggests that a privacy policy must “address” third party disclosure, private information security measures, and email usage.
26	Frequency and means of updates to scheme	None stated.

27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	Privacy seal can be bundled with a security seal, which requires meeting PCI security scanning – a daily vulnerability scan, and is using 128-bit SSL encryption on pages where private information may be entered.
28	Complaints mechanism	Via “Contact us” information in a web form.
29	Criticisms	<ul style="list-style-type: none"> • The Trustify-me website doesn’t provide identity information or contact details for Trustify-me itself, whilst talking about the importance of these details for other websites. • Trustify-me appears to have little impact, and few subscribers. The standards required for a seal are minimal and vague. There is poor information on the scheme, and no contact details for the scheme’s administrators.
30	Links and references to the scheme	<ul style="list-style-type: none"> • None.
31	Logo	 The logo for Trustify-Me Privacy Certified. It features a globe icon on the left. To the right of the globe, the text 'Trustify-Me' is written in a large, bold, sans-serif font, with 'Privacy Certified' underneath it in a smaller font. Above the globe, the URL 'http://trustify-me.org' is written in a small font. Below the globe, the text 'Seal Passed: 02-04-2012' is written in a small font.
32	Website	http://trustify-me.org
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	Not stated.
34	Data collection for specified, explicit and legitimate purposes	Not stated.
35	Adequate, relevant and limited data collection	Not stated.
36	Data accuracy	Not stated.
37	Time and purpose restricted data retention	Not stated.
38	Data is processed under the responsibility and liability of the controller	Not stated.
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not stated.
40	Consent requirement for processing of special personal data	Not stated.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Not stated.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Not stated.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Not stated.
44	Provision for communication of rectification or	Not stated.


	erasure carried out under Articles 16 and 17	
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	Not stated.
46	Provision for right of access for the data subject	Not stated.
47	Provision for right to rectification	Not stated.
48	Provision for right to be forgotten and to erasure	Not stated.
49	Provision for right to data portability	Not stated.
50	Provision for data subject's right to object	Not stated.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not stated.
52	Rights in relation to automated processing	Not stated.
53	Documentation requirements (Art 28)	Website must have a privacy policy in order to qualify for the Trusty-me privacy certification seal.
54	Implementing the data security requirements (Article 30)	Not stated.
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not stated.
56	Communication of a personal data breach to the data subject (Article 32)	Not stated.
57	Data protection impact assessment (Article 33)	Not stated.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not stated.
59	Designation of a data protection officer (Article 35(1))	Not stated.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	Not stated.

11.23 TÜV TRUSTED SITE PRIVACY CERTIFICATION MARK

	General criteria for evaluation and comparison of privacy seals	TÜV Trusted Site Privacy certification mark
1	Nature (privacy-oriented/general trust mark)	Privacy certification mark.
2	Country	Germany.
3	Inception	The TÜViT TSPPrivacy Certification Scheme started in 2006 and the first certificate was issued in 2006.
4	Issuing organisation	TÜV Informationstechnik GmbH
5	Issuer type	Testing, certification, auditing and consulting company
6	Target of scheme	IT procedures, organisations and parts of organisations (data protection management systems).
7	Number of certified entities	According to TÜViT, it has issued about 12 certificates, mostly for IT-systems, such as the rating and billing processes of Deutsche Telekom or the secure electronic mailing- E-Postbrief - of Deutsche Post.
8	Renewals	-
9	Types of entities that can be certified	IT companies, organisations
10	Type of beneficiaries	Users of IT services
11	Objective of scheme	To provide proof of privacy conformity.
12	Descriptive summary of scheme	According to the website : The Trusted Site Privacy certification mark is given for IT procedures, organisations and parts of organisations (data protection management systems) and is based on the assessment by the TÜViT data protection evaluation body. The assessment of the data privacy is based on a comprehensive and legally-compliant test approach. Among other things, the ‘quid! Criteria’ (which were developed in a two-year EU research project quid! with more than 80 experts) are used to assess quality in company data protection. The criteria were developed in a two-year research project with more than 80 experts and provide the core requirements for the Trusted Site Privacy criteria list .
13	Unique selling point	According to the TÜViT document <i>Certification procedure for data protection concepts and IT systems- Trusted Site Privacy 2013</i> , “the evaluation of the data protection of IT systems and IT processes cannot be implemented based on legislation alone. It is absolutely essential- following determination of the privacy requirements and starting from the relevant legislation - also to investigate and assess the relevant organisational and technical measures involved. Data protection and IT security complement each other here and are directly dependent upon one another.”
14	Privacy/data protection elements of the scheme	Data processing, data subject rights, transparency, data protection documentation, technical and organisational measures, data protection management

15	Guarantees offered to the data subject	According to a TÜViT communication (email dated 27.05.13), they “provide no special guarantees to data subjects.” TÜViT certifies conformity with the Trusted Site Privacy criteria, which is based on the applicable law for a concrete use scenario of a Target of Audit (the system to be certified).
16	Steps in the certification process	<p>According to the TÜViT <i>Certification procedure for data protection concepts and IT systems- Trusted Site Privacy Version 2.9, 2013</i>, the aspects of evaluation are: a data protection audit and a security-related investigation.</p> <p>Steps in the process:</p>  <pre> graph TD subgraph Stage1 [1 Certification Body Audit Controlling] A["„As Is“ Analysis Checklist - Kick-off meeting - Workshop"] B["Specification Object of Audit/Scope of Attestation, Types of data processed, Qualification Targets"] A --> B end subgraph Stage2 [2 Team of legal & technical experts] C["Review of Documentation Data Protection Concept, Product Documentation"] D["Data Protection Audit / Security Inspection / Product and Service Test"] B --> C C --> D end subgraph Stage3 [3 Certification Body] E["Inspection Report technical, legal aspects"] D --> E end E --> F["Certificate"] F --> G["Re-Certification"] G --> B </pre>
17	Coverage of international transfers	Not specified on list available online .
18	Costs (i.e., evaluation cost, certification cost)	According to a TÜViT communication (email dated 27.05.13), the expenses of evaluation and certification fee depend on the IT-complexity of the system or process to be certified and these costs are individually calculated each time. If there is for instance a “small” Target of Audit the effort will be about 30 person days plus certification fee of about €4.470.
19	Validity	The certification is valid for two years and can be renewed.
20	Revocation mechanism	<p>TÜViT, Certification Conditions for Test Mark Usage of the Certification Body TÜV Informationstechnik GmbH, Version 2009:</p> <p>The certification body has the right to suspend a certificate and to suspend the right of the client to use the test mark, if new findings relevant for the evaluation of the results of the certification process will be known. In this case the certification body offers the client a re-certification of the product. In the case that re-certification is not successful</p>

		the certificate can be withdrawn. The client is obliged not to use a suspended certificate and its corresponding test mark until the final decision of the certification body. This means, that during the suspension period no misleading sayings considering the certification status of the product must be done. In addition, a certification label or test mark must not be attached to the product or used in documents referring to this product.
21	Recognition	According to TÜViT, the quid! criteria were worked out by more than 80 experts from industry and science, from state and private data protection organizations, from public administration bodies, consultancy organisations, from federations and trade unions and from works councils and top company management within the two-year EU quid! research project. The TÜViT Data Protection Evaluation Centre is accredited to carry out other privacy certification evaluations. TÜViT is recognised by ULD (Independent Center of Privacy Protection Schleswig-Holstein, Germany - Office of the Privacy Protection Commissioner of Schleswig-Holstein) for the privacy mark: Datenschutz-Gütesiegel and for European Privacy Seal (https://www.european-privacy-seal.eu/). It is accredited by the German Data Protection Officer to provide data protection proof for the accreditation of De-Mail service providers in accordance with § 18 Para. 3 of the De-Mail Act regarding the German communication services regulated by law.
22	Accredited experts and/or evaluation bodies	Currently there are no external experts accredited for the Trusted Site Privacy Certification.
23	Duration and scope of the certification process	According to a TÜViT communication (email dated 27.05.13), the duration of the certification process depends of the complexity of the Target of Audit and the quality of the customer documentation. A small certification takes about 3 months.
24	Number of certified experts and/or bodies	Only employees of TÜViT are involved.
25	Regulatory/ compliance standards	Trusted Site Privacy criteria
26	Frequency and means of updates to scheme	According to TÜViT, only when it is required by legal changes.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	Includes a security component.
28	Complaints mechanism	TÜViT, <i>Certification Conditions for Test Mark Usage of the Certification Body TÜV Informationstechnik GmbH</i> , Version 2009: The client is obliged to record all complaints by a third party with respect to the properties of the product which are confirmed by the certificate and all resulting measures. On request, this documentation must be made available to the certification body. The client must immediately take necessary counter measures imposed by the complaints and

		keep a record of the whole proceedings. The certification body must also be informed immediately about these proceedings to be able to judge about possible implications on the certification statement.
29	Criticisms	
30	Links and references to the scheme	<ul style="list-style-type: none"> Jentzsch, Nicola “Was können Datenschutz-Gütesiegel leisten?”, <i>Wirtschaftsdienst</i>, June 2012, Vol. 92, Iss. 6, pp. 413-419.
31	Logo	 <p>The logo features a red square with the word 'Privacy' in white, a black square with '2013' in white, and a black square with 'Trusted Site' in white. To the right is the 'TUVIT' logo in black with a red swoosh, and below it 'Voluntary Validation' and '© TÜVIT - Member of TÜV NORD Group'.</p>
32	Website	https://www.tuvit.de/en/privacy/uld-privacy-seal-1075.htm
General data protection regulation requirements under Ch II and III		
33	Fair, lawful, transparent processing of personal data	The Trusted Site Privacy criteria require legal compliance of each phase of data processing and observance of principles of data protection regulations regarding data processing on behalf of a controller.
34	Data collection for specified, explicit and legitimate purposes	The Trusted Site Privacy criteria speak of the legitimacy of data processing and legal compliance of each phase of data processing.
35	Adequate, relevant and limited data collection	<p>The Trusted Site Privacy criteria call for fulfilment of the basic principles of data protection and privacy so would be implied.</p> <p>The TÜViT document “Certification procedure for data protection concepts and IT systems- Trusted Site Privacy” Version 2.9, 2013 specifies that “Requirements regarding data economy, i.e. to ensure that only essential data is collected, are taken into consideration in association with the state of technology”.</p>
36	Data accuracy	The Trusted Site Privacy criteria call for fulfilment of the basic principles of data protection and privacy, so would be implied.
37	Time and purpose restricted data retention	The Trusted Site Privacy Criteria call for fulfilment of the basic principles of data protection and privacy, so would be implied.
38	Data is processed under the responsibility and liability of the controller	Not specified as such but criteria cover responsibility for data protection.
39	Provision for parental consent based processing of personal data of a child below the age of 13	-
40	Consent requirement for processing of special personal data	Would be covered under the fulfilment of the basic principles of data protection and privacy.
41	Transparent and easily accessible policies on processing of personal	The Trusted Site Privacy criteria specify transparency of the privacy and data protection policy and transparency of

	data and for the exercise of data subjects' rights.	data privacy documentation.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Complex 2 of the Trusted Site Privacy criteria speaks of transparency and friendliness to data subjects.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	The Trusted Site Privacy criteria specify respect for the rights of data subjects and support of data subjects in the assertion of their rights.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	The Trusted Site Privacy criteria specify respect for the rights of data subjects and support of data subjects in the assertion of their rights.
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data is stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients personal data • Transfer to a third country or international organisation and on the adequacy of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	Complex 2 of the Trusted Site Privacy criteria specifies transparency and friendliness to data subjects. No further details provided.
46	Provision for right of access for the data subject	The Trusted Site Privacy criteria broadly specify support of data subjects in the assertion of their rights
47	Provision for right to rectification	Not specified.
48	Provision for right to be forgotten and to erasure	Not specified.
49	Provision for right to data portability	Not specified.
50	Provision for data subject's right to object	The Trusted Site Privacy criteria broadly specify support of data subjects in the assertion of their rights
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not specified.
52	Rights in relation to automated processing	Not specified.
53	Documentation requirements (Art	The Trusted Site Privacy criteria specify documentation of

	28)	the data protection measures.
54	Implementing the data security requirements (Article 30)	The Trusted Site Privacy criteria specify technical security and specific, organisational requirements regarding the target of evaluation.
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not specified.
56	Communication of a personal data breach to the data subject (Article 32)	Not specified.
57	Data protection impact assessment (Article 33)	The Trusted Site Privacy criteria (under data protection management) specify risk analysis, regular inspections for improvement of the data protection measures, and continual improvement process.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not specified.
59	Designation of a data protection officer (Article 35(1))	The Trusted Site Privacy criteria outline functional conditions of the data protection officer.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	Not specified.


11.24 VERIFIED BY VISA

	General criteria for evaluation and comparison of privacy seals	Verified by Visa
1	Nature (privacy-oriented/general trust mark)	Protection of online payments scheme
2	Country	International (some variations in local jurisdictions)
3	Inception	2001
4	Issuing organisation	Visa
5	Issuer type	Private company/bank
6	Target of scheme	Online retailers, banks, bank customers
7	Number of certified entities	300,000 websites across Europe. 10,000 issuers, more than 250 million pre-registered cardholders.
8	Renewals	Re-certification is necessary if a merchant switches to new payments software, changes payments processor or installs software updates that significantly alter their payments software.
9	Types of entities that can be certified	Online retailers, banks and card issuers
10	Type of beneficiaries	<p>Online retailers (fewer rejected or queried sales, fewer refunds), banks (less online card fraud, bank branding associated with online transactions), individual customers (reduced exposure to fraud, reduction in unauthorised use of credit/debit cards).</p> <p>Merchants who implement Verified by Visa get transactions treated as cardholder-present transactions with much less risk of repudiation, while banks get to shift liability for fraudulent transactions to customers, as a password has been used. The merchant is protected against cardholder denying making a purchase.</p>
11	Objective of scheme	To protect credit and debit cards against unauthorised use in online transactions and give users confidence that an online retailer has made security a priority.
12	Descriptive summary of scheme	Verified by Visa allows participating online retailers to offer an additional password protected stage to online card transactions. The retailer hosts an inline frame redirecting the customer to their card-issuing bank, to provide additional information (a number of letters or digits from a longer password) before authorising the transactions. This provides the retailer with an authorisation code they can later provide to the bank. This is claimed to provide greater security for the card user. The way that a user signs up for the process (and resets passwords) is left to the discretion of the card issuing bank, but often occurs during an online transaction. Some banks mandate that card users sign up for Verified by Visa if they wish to conduct

		<p>online transactions.</p> <p>The full process works if the card holder has signed up for the service with their card issuer, and the online merchant has also signed up to offer the service, through their payments service provider.</p> <p>The key benefits appear to be to shift liability away from the merchant for card-not-present transactions, regardless of if the cardholder has enrolled with the card issuer or not. The scheme has been criticised for not actually providing substantial security benefits to the customer, but primarily benefiting the bank and the merchants.</p>
13	Unique selling point	<p>The scheme intends to help decrease the risk of merchants reusing card details, as the password is not revealed to the merchant during the transaction. The use of the password also means that card details copied from the physical card cannot be used to make purchases online. Verified by Visa enables issuing banks to authenticate the identity of any card holders enrolled in the service when making transactions over the Internet.</p> <p>Mastercard SecureCode, JCB International J/Secure, and American Express SafeKey are almost functionally identical to Verified by Visa, and are based upon the same 3-D Secure protocol. Many payment service providers offer the possibility to install functionality for all of these at the same time.</p>
14	Privacy/data protection elements of the scheme	<p>Visa Privacy Policy - http://www.visaeurope.com/en/site_services/privacy.aspx</p> <p>Individual Card issuer privacy policies.</p> <p>Payment Card Industry Data Security Standard (PCI DSS) is required of all entities that store, process or transmit Visa cardholder data. This includes building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management programme, implementing strong access controls, regularly monitoring and testing networks, and maintaining an information security policy.</p>
15	Guarantees offered to the data subject	<p>Apparently none – the scheme does not guarantee any greater security. There are no additional privacy guarantees.</p> <p>Furthermore, according to its website, “The Service does not give you any extra rights regarding the quality or fitness for purpose of the goods or services that you purchase. You should always</p>

		make sure that you make your online purchases from reputable retailers.”
16	Steps in the certification process	<p>Cardholders register for the services and choose a private password for use when shopping online at a participating retailer.</p> <p>Retailers enrol into the service and make enhancements to their check out or payment processes on their website. Merchants must have operational and certified 3-D Secure software on their web sites as a Merchant Plug in (MPI). Merchants generally enrol through their Electronic Funds Transfer software provider, Payment Service Provider or MPI vendor.</p> <p>The certification process in the US also includes Payment Card Industry Data Security Standards (PCI DSS) compliance, PIT (product integration testing).</p> <p>Where testing is required it takes the form of a three stage process:</p> <ol style="list-style-type: none"> 1. MasterCard and/or Visa must confirm that a merchant’s chosen Merchant Plug-In (MPI) is compliant to their latest software version. 2. The respective card scheme tests the functionality of the merchant’s MPI 3. The output of the merchant’s Electronic Funds Transfer (EFT) software is tested to ensure that the correct data is being included at the Authorisation stage. <p>The implementation and testing of the MPI take place with the chosen vendor who must provide a Letter of Compliance confirming that their software has under gone the required test process with Visa.</p> <p>The Visa PIT is designed to be an automated, self-testing facility whereby testers enrol and perform testing with minimum interaction from PIT administrators (i.e. users must self-certify successful completion). PIT automatically evaluates the results.</p>
17	Coverage of international transfers	Businesses taking transactions within the EU region from cards issued outside of the EU will not benefit from the liability shift.
18	Costs (i.e., evaluation cost, certification cost)	<p>Generally paid for by the merchant as an outsourced service. The cost to purchase the required software is \$2,000 with annual maintenance payments.</p> <p>No costs levied by VISA for automated functionality testing</p>
19	Validity	Valid once appropriate software is installed and tested and the license agreement is signed with service provider.

20	Revocation mechanism	<p>No information given. If the relationship with financial service provider is terminated, then the use of Verified by Visa through that service provider would also end.</p> <p>The Visa PCI DSS states, “If a member, merchant or service provider does not comply with the security requirements or fails to rectify a security issue, Visa may fine the responsible member. Visa may waive fines in the event of a data compromise if there is no evidence of non-compliance with PCI DSS and Visa rules. To prevent fines a member, merchant, or service provider must maintain full compliance at all times, including at the time of breach as demonstrated during a forensic investigation. Additionally, a member must demonstrate that prior to the compromise the compromised entity had already met the compliance validation requirements, demonstrating full compliance.”</p>
21	Recognition	<p>Visa holds a significant market share in card payments (as does MasterCard) and is internationally recognised.</p>
22	Accredited experts and/or evaluation bodies	-
23	Duration and scope of the certification process	<p>Receiving digital certificates from Visa may take approximately two weeks. MPI vendors may already have these and be able to implement Verified by Visa upon a client’s web store very rapidly.</p>
24	Number of certified experts and/or bodies	Not clear.
25	Regulatory/ compliance standards	<p>Banks must use compatible software. Merchants must meet the set of technical requirements in the Acquirer and Merchants Implementation Guide, which include technical details, security standards, training for customer support, and the appearance of Verified by Visa branding. Merchants must also comply with the Visa Operating Regulations. Merchants in the US must be CISP compliant (Cardholder Information Security Plan).</p> <p>Banks also apply terms and conditions of using a credit or debit card onto the customer.</p>
26	Frequency and means of updates to scheme	<p>Not specified on Visa website. Banks across Europe are running trial and pilots of new versions of the scheme, including Dynamic Passcode Authentication and the Visa CodeSure card.</p>
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	None specified.
28	Complaints mechanism	<p>No complaints mechanism solely for Verified by Visa. Complaints can be directed towards card issuers, individual merchants or Visa Europe.</p>

29	Criticisms	<ul style="list-style-type: none"> • It is hard for users to distinguish between a legitimate Verified by Visa window and a man-in-the-middle attack. • The scheme is potentially insecure and promotes insecure behaviour. • It imposes new terms on conditions on the user without appropriate consent mechanisms and is imposed by banks on unwilling consumers. • It shifts liability for fraudulent transactions onto the user. • It provides less privacy for the user than previous payments or single-sign on mechanisms. • It may also prevent mobile payments if card issuer has not addressed this issue.
30	Links and references to the scheme	<ul style="list-style-type: none"> • Brignall, Miles, “Verified by Visa Scheme confuses thousands of internet shoppers”, <i>The Guardian</i>, 21 April 2007. http://www.guardian.co.uk/money/2007/apr/21/creditcards.debt • Murdoch, Steven J. & Ross Anderson, “Verified by Visa and Mastercard SecureCode: Or, How Not to - Design Authentication”, in R. Sion (ed), <i>Financial Cryptography and Data Security</i>, LNCS 6052, 2010, pp. 336–342. • Ferguson, Rik, “Verified by Visa?”, <i>Countermeasures, Security, Privacy and Trust</i>, A Trend Micro blog, 1 Dec 2011. http://countermeasures.trendmicro.eu/Verified by Visa /
31	Logo	
32	Website	https://usa.visa.com/personal/security/vbv/index.jsp and http://www.visa.co.uk/en/security/online_security/verified_by_visa.aspx
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	Not stated.
34	Data collection for specified, explicit and legitimate purposes	Not stated.
35	Adequate, relevant and limited data collection	Not stated.
36	Data accuracy	Not stated.
37	Time and purpose restricted data retention	PCI DSS standards require keeping cardholder data to a minimum by implementing data retention and disposal policies, procedures and process. It includes limiting data storage amount and retention

		time to that required for legal, regulatory and business requirements, processes for secure deletion of data when no longer needed and quarterly processes for identifying and deleting stored cardholder data that exceeds defined retention requirements.
38	Data is processed under the responsibility and liability of the controller	PCI DSS standards require limiting access to system components and cardholder data only to those individuals whose job requires such access.
39	Provision for parental consent based processing of personal data of a child below the age of 13	Not Stated. Verified by Visa is not targeted at children under 13.
40	Consent requirement for processing of special personal data	Not stated.
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	Not easily accessible, poor information on the exercise of data subject rights.
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	Visa website provides relatively limited information on processing of personal data. Customers and merchants are directed towards their own bank for further information. PCI DSS standards that underpin the data protection aspects of Verified by Visa require some effort to access.
43	Existence of procedures and mechanisms for exercising the rights of the data subject	Not stated.
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	Not stated.
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequate decision by the Commission • Any further information necessary to guarantee fair processing 	Little information about the security and privacy component of the scheme is easily accessible to the data subject. Privacy policies often refer to the use of data collected by Visa websites.
46	Provision for right of access for the data subject	Not stated.
47	Provision for right to rectification	Not stated.
48	Provision for right to be forgotten and to erasure	Not stated.
49	Provision for right to data portability	Not stated.
50	Provision for data subject's right to object	Not stated. Several card issuers make using 'Verified by Visa' a condition of using that card for


		payment at participating merchants and allow only a limited number of opt outs before customer registration becomes mandatory.
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	Not stated.
52	Rights in relation to automated processing	Not stated.
53	Documentation requirements (Art 28)	Not stated.
54	Implementing the data security requirements (Article 30)	PCI DSS security standards must be implemented by merchants enrolling for Verified by Visa, and include access control and data security requirements.
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not stated.
56	Communication of a personal data breach to the data subject (Article 32)	Not stated.
57	Data protection impact assessment (Article 33)	Not directly stated, although the PCI DSS standards require documented information security risk assessment process.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	Not stated.
59	Designation of a data protection officer (Article 35(1))	PCI DSS standards require assigning individual or team information security responsibilities that overlap with some data protection officer functions.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	Not stated.

11.25 WEBTRUST PRIVACY SEAL

	General criteria for evaluation and comparison of privacy seals	WebTrust Privacy Seal
1	Nature (privacy-oriented/general trust mark)	Privacy seal
2	Country	USA/Canada
3	Inception	1998
4	Issuing organisation	Chartered accountants and chartered public accountants licensed by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Chartered Public Accountants (AICPA).
5	Issuer type	Chartered accountants and chartered public accountants licensed by the CICA and the AICPA.
6	Target of scheme	Practitioners and clients.
7	Number of certified entities	Data not found.
8	Renewals	-
9	Types of entities that can be certified	E-commerce-based systems.
10	Type of beneficiaries	Web users, consumers, businesses.
11	Objective of scheme	To signify “that the client’s policies, communications, procedures and monitoring efforts support the ten integral components of the Privacy Principle: management accountability; notice of privacy policies; choice and consent for individuals; collection of personal information; use and retention of personal information; access to personal information; disclosure to third parties; security; quality of personal information; and monitoring and enforcement”. (AICPA/CICA International Seal Usage Guide 2004).
12	Descriptive summary of scheme	The WebTrust seal can be obtained by engaging a chartered accountant or a chartered public accountant to certify that a business complies with the WebTrust Principles and Criteria for the specific WebTrust seal sought by the business entity.
13	Unique selling point	<ul style="list-style-type: none"> • Full information systems audit by a public accountant is required to obtain the seal. • Annual audit for compliance by a third party, licensed professional.
14	Privacy/data protection elements of the scheme	Management accountability, notice of privacy policies, choice and consent for individuals, collection of personal information, use and retention of personal information, access to personal information, disclosure to third parties, security, quality of personal information and monitoring and enforcement.
15	Guarantees offered to the data subject	Personal information is collected, used, retained, and disclosed, and disposed of in conformity with the commitments in the entity’s privacy notice and with

		criteria set forth in Generally Accepted Privacy Principles issued by the AICPA/CICA.
16	Steps in the certification process	Practitioners may provide the seal to clients after: 1) The practitioner completes an assessment based on the Trust Services Principles and Criteria. 2) The client's system receives an unqualified attestation report. 3) The practitioner pays the seal management fee on behalf of the client. 4) The client agrees to the Seal Usage Guidelines .
17	Coverage of international transfers	Not covered.
18	Costs (i.e., evaluation cost, certification cost)	The cost varies according to the ability to adhere to the WebTrust standards. The AICPA/CICA International Seal Usage Guide 2004 pegged the cost of seals issued to clients in the US and Canada at \$1,500 USD and \$1,500 CAD per seal respectively.
19	Validity	One year, plus a 90-day grace period, unless revoked or suspended. The grace period is provided to allow sufficient time for completing the follow-up review.
20	Revocation mechanism	If the practitioner determines that a client's systems, policies and disclosures fail to comply with the Trust Services Principles and Criteria at any time or if the client fails to renew the seal through a follow-up review at the end of one year, the practitioner will immediately notify the client and advise that the seal must be removed from the client's web site and any printed or online materials. The practitioner will suspend all the relevant links from the active Trust Services web site using the Seal Management System and notify the local institute of certified public accountants or equivalent. The practitioner may restore a seal after revocation or suspension if an unqualified report can be rendered. The practitioner may either reinstate the original report if it is once again accurate or issue a new report.
21	Recognition	The WebTrust seal is widely recognised by the public and other businesses in US and Canada and globally.
22	Accredited experts and/or evaluation bodies	Chartered accountants and chartered public accountants licensed by the CICA and the AICPA. WebTrust also has a program for certification authorities.
23	Duration and scope of the certification process	Duration: Not specified. Scope: The WebTrust Privacy Seal provides visual verification that a client's e-commerce system safeguards the user's privacy by protecting personal information. The seal signifies that the client's policies, communications, procedures and monitoring efforts support the ten integral components of the Privacy

		Principles: management accountability, notice of privacy policies, choice and consent for individuals, collection of personal information, use and retention of personal information, access to personal information; disclosure to third parties, security, quality of personal information and monitoring and enforcement.
24	Number of certified experts and/or bodies	A list of global practitioners is available at: http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx
25	Regulatory/ compliance standards	WebTrust principles and related criteria developed by the AICPA and the CICA, specifically the Generally Accepted Privacy Principles (GAPP) , a comprehensive privacy framework aimed at assisting businesses create an “effective privacy program that addresses privacy risks and business opportunities”. The AICPA and CICA jointly developed the GAPP framework and it is founded on single privacy principle supported by 10 principles and more than 70 objectives and measurable criteria.
26	Frequency and means of updates to scheme	GAPP was updated in August 2009.
27	Additional elements (e.g., security or other components, links with a privacy program (privacy audits, awareness))	WebTrust also offers other seals such as WebTrust Security Seal, WebTrust Processing Integrity Seal, WebTrust Availability Seal, WebTrust Confidentiality Seal, WebTrust Consumer Protection Seal, and WebTrust® for Certification Authorities.
28	Complaints mechanism	Not found on website. According to a study by the SANS Institute : Complaints can be initiated with the National Arbitration Forum via the Internet, telephone or the regular mail. It costs \$49 for claims less than \$1,000 and between \$49- \$150 for claims greater than \$1,000. The losing party pays the costs. Most disputes are typically resolved within 45-60 days, If one of the parties is not satisfied with the NAF’s decision, the party can still go to court.
29	Criticisms	<ul style="list-style-type: none"> • Higher evaluation costs due to extensive review process. • Cost associated with complaints.
30	Links and references to the scheme	<ul style="list-style-type: none"> • Hiller, Janine S., and France Belanger, “Privacy strategies for electronic government”, <i>E-government</i> 200, 2001, pp. 162-198. • Moores, Trevor T., and Gurpreet Dhillon, “Do privacy seals in e-commerce really work?” <i>Communications of the ACM</i>, Vol. 46, No. 12, 2003, pp. 265-271. • Shapiro, Brian and C. Richard Baker, “Information technology and the social construction of information privacy”, <i>Journal of Accounting and Public Policy</i>, Vol. 20, No. 4, 2002, pp. 295-322. • Kovar, Stacy E., K. G. Burke, Brian R. Kovar, “Selling WebTrust: An exploratory examination

		of factors influencing consumers' decisions to use online distribution channels", <i>The Review of Accounting Information Systems</i> , Vol. 4, No 2.
31	Logo	<p style="text-align: center;">Privacy</p>  <p style="text-align: center;">Practitioner Firm's Name</p>
32	Website	http://www.webtrust.org
	General data protection regulation requirements under Ch II and III	
33	Fair, lawful, transparent processing of personal data	GAPP Collection criteria 4.2.2 speaks of collection by fair and lawful means i.e. that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.
34	Data collection for specified, explicit and legitimate purposes	GAPP Collection criteria 4.2.1 - Collection Limited to Identified Purpose - The collection of personal information is limited to that necessary for the purposes identified in the notice.
35	Adequate, relevant and limited data collection	GAPP Collection criteria 4.2.1 - Collection Limited to Identified Purpose - The collection of personal information is limited to that necessary for the purposes identified in the notice.
36	Data accuracy	GAPP Quality criteria 9.0 states: The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
37	Time and purpose restricted data retention	GAPP Use, Retention, and Disposal Criteria 5.0 states: The entity retains personal information for only as long as necessary to fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
38	Data is processed under the responsibility and liability of the controller	<i>GAPP additional consideration</i> under 7.2.2: The entity is responsible for personal information in its possession or custody, including information that has been transferred to a third party.
39	Provision for parental consent based processing of personal data of a child below the age of 13	GAPP Use, Retention, and Disposal Criteria 5.2.1 on the use of personal information specifies: Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise. This implies acting in line with the requirements of the Children's Online Privacy Protection Act (COPPA).

40	Consent requirement for processing of special personal data	<p>GAPP criteria 3.2.3 <i>Explicit Consent for Sensitive Information</i> states that explicit consent must be obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise. Sensitive personal information is defined in the GAPP document as “personal information that requires an extra level of protection and a higher duty of care, for example, information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions”.</p>
41	Transparent and easily accessible policies on processing of personal data and for the exercise of data subjects' rights.	<p>GAPP criteria 1.0 specifies that an entity must define, document, communicate, and assign accountability for its privacy policies and procedures with respect to: notice, choice and consent, collection, use, retention, and disposal, access, disclosure to third parties, security for privacy, quality, monitoring and enforcement.</p> <p>GAPP criterion 1.1.0 requires that privacy policies are documented in writing and made readily available to internal personnel and third parties who need them.</p> <p>GAPP criterion 2.2.1 (illustrative controls) clarifies that the privacy notice must be: readily accessible and available when personal information is first collected from the individual; provided in a timely manner (i.e., at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information to the entity; and clearly dated to allow individuals to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity.</p>
42	Intelligible, clear information, communication relating to the processing of personal data to the data subject, in particular for any information addressed specifically to a child.	<p>The GAPP Notice criterion 2.0 specifies that an entity must provide notice about its privacy policies and procedures and identify the purposes for which personal information is collected, used, retained, and disclosed.</p> <p>GAPP criterion 2.2.3 specifies that the entity’s privacy notice must be conspicuous and use clear language.</p>
43	Existence of procedures and mechanisms for exercising the rights of the data subject	<p>GAPP Access criterion 6.0 specifies that the entity provide individuals with access to their personal information for review and update.</p>
44	Provision for communication of rectification or erasure carried out under Articles 16 and 17	-
45	Provision of information to data subject: <ul style="list-style-type: none"> • identity and the contact details of the controller • purposes/conditions of the processing 	Covered in the GAPP Notice criterion. 2.2.1 deals with communication to individuals (it suggests the entity’s privacy notice describe the personal information collected, the sources of such information, purposes for which it is collected, indicate the purpose for collecting

	<ul style="list-style-type: none"> • Period for which the personal data will be stored • Existence of the right to request access to and rectification or erasure • Right to lodge a complaint to the supervisory authority • Recipients, categories of recipients of personal data • Transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission • Any further information necessary to guarantee fair processing 	<p>sensitive personal information and whether such purpose is part of a legal requirement, describe the consequences, if any, of not providing the requested information, indicate that certain information may be developed about individuals, such as buying patterns etc). GAPP criterion 2.2.2. elaborates that privacy notices provide an objective description of the entities and activities covered by the privacy policies and procedures.</p> <p>GAPP criterion 6.1.1 on communication to individuals states that individuals must be informed about how they may obtain access to their personal information to review, update, and correct that information.</p>
46	Provision for right of access for the data subject	GAPP <i>Access</i> criterion 6.0 specifies that the entity provide individuals with access to their personal information for review and update.
47	Provision for right to rectification	GAPP criterion 6.2.5 deals with updating or correcting personal information. Individuals can update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.
48	Provision for right to be forgotten and to erasure	GAPP criterion 5.2.3 deals with the disposal, destruction and redaction of personal information. Personal information no longer retained is anonymised, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorised access.
49	Provision for right to data portability	-
50	Provision for data subject's right to object	-
51	Right to object free of charge to the processing of their personal data in cases of direct marketing (explicit offering of right)	-
52	Rights in relation to automated processing	-
53	Documentation requirements (Art 28)	-
54	Implementing the data security requirements (Article 30)	<p>GAPP criterion 8.0 specifically focuses on <i>security for privacy</i>. It states that "the entity protects personal information against unauthorized access (both physical and logical)".</p> <p>GAPP criterion 8.1.0 suggests privacy policies address security of personal information; GAPP criterion 8.1.1 suggests individuals must be informed that precautions</p>

		are taken to protect personal information. GAPP criterion 8.2.2 calls for the development of a comprehensive Information Security Program. GAPP criterion 8.2.2 deals with Logical Access Controls; criterion 8.2.3 deals with Physical Access Controls and criterion 8.2.4 deals with Environmental Safeguards. GAPP criterion 8.2.5 calls for protection of Transmitted Personal Information. GAPP criterion 8.2.6. calls for protecting of personal information stored on portable media or devices from unauthorized access. GAPP criterion 8.2.7 deals with testing security safeguards.
55	Notification of a personal data breach to the supervisory authority (Article 31)	Not specified as such, though GAPP criterion 1.2.7 has detailed provisions on Privacy Incident and Breach Management.
56	Communication of a personal data breach to the data subject (Article 32)	GAPP criterion 1.2.7 specifies a stakeholders breach notification. If required by law, regulation, or policy, the entity must have a process for delivering the breach notice in a timely manner. GAPP criterion 10.2.1 speaks of remedies to be available in case of a breach of personal information and how to communicate this information to an individual.
57	Data protection impact assessment (Article 33)	GAPP Management criterion 1.1.6 specifies: The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies.
58	Compliance with the requirements for prior authorisation/ prior consultation of the supervisory authority pursuant to Article 34(1) and (2)	-
59	Designation of a data protection officer (Article 35(1))	GAPP criterion 1.1.2 <i>Responsibility and Accountability for Policies</i> specifies: Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.
60	Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations	GAPP criterion 10.0 states that an entity must monitor compliance with its privacy policies and procedures and have procedures to address privacy related inquiries, complaints and disputes. GAPP criterion 10.2.3 specifies a compliance review (a review and documentation of compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts, with results of such reviews reported to management and remediation plans for problems).

		<p>GAPP criterion 10.2.5 deals with ongoing monitoring which include action such as: control reports, trend analysis, training attendance and evaluations, complaint resolutions, regular internal reviews, internal audit reports, independent audit reports covering controls at service organisations and other evidence of control effectiveness.</p>
--	--	---

12 ANNEX II – “FINGERPRINTS” OF INDIVIDUAL SEAL SCHEMES

This Annex presents the “fingerprints” of each analysed certification scheme.

12.1 BBB ACCREDITED BUSINESS SEAL

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	scale (very large/ large/ medium/ small)	certifies	accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	Medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.2 BUYSAFE GUARANTEED SHOPPING

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	scale (very large/large/medium/small)	certifies	accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	Medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.3 CLOUD SECURITY ALLIANCE

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.4 CNIL LABEL

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.5 COMODO SECURE

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for-Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.6 CONFIANZA ONLINE

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.7 DANISH E-MARK

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.8 EPRIVACYSEAL

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.9 ESRB PRIVACY ONLINE CERTIFICATION

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for-Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.10 EURO-LABEL

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.11 EUROPRiSE (EUROPEAN PRIVACY SEAL)

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.12 GIGYA'S SOCIALPRIVACY™ CERTIFICATION

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.13 MARKET RESEARCH SOCIETY (MRS) FAIR DATA

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.14 MCAFEE SECURE

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information Security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.15 PRIVACYMARK SYSTEM

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.16 PRIVO PRIVACY CERTIFIED

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.17 SERIEDAD ONLINE

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.18 SMART GRID PRIVACY SEAL

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.19 TRANSACTION GUARD PRIVACY POLICY VERIFIED SEAL

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.20 TRUSTE

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.21 TRUSTED SHOPS

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.22 TRUSTIFY-ME PRIVACY CERTIFICATION SEAL

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.23 TÜVIT TRUSTED SITE PRIVACY

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of members			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.24 VERIFIED BY VISA

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information Security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

12.25 WEBTRUST

Model	Nature	Certification assessment	Country	Issuer type	Data protection and privacy elements	Guarantees	Complaints	Scale (very large/large/medium/small)	Certifies	Accredited experts (yes/no)
Classic Seal	General	Standards	Global	Private company	None	None specific	Unknown	Small	Organisations	Yes
Linked Seal	Privacy Seal	Service	United States (International)	Data protection authority	Abstract	Abstract	Contact email only	medium	Websites	No
Hosted Seal	E-Commerce	Consultant	United States (Domestic)	Not-for Profit/non-governmental organisation	Legally Aligned	Compliance with law	Member first	Large	Systems	
External Standards seal	Security		Canada	Professional representative body (industry association)	Detailed	Detailed	Scheme first	Very large		
Delegated Certification Seals			Europe		Granular	Highly granular	Required of member			
Federated Seals			France		Information security	Financial				
Security Scan seals			United Kingdom							
Insurance Seals			Spain							
Registry (Self-assessment)			Denmark							
Registry (investigative)			Germany							
3-D Secure			Japan							

European Commission
EUR 26190 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: EU Privacy seals project

Author(s): Rowena Rodrigues, David Barnard-Wills, David Wright, Paul De Hert, Vagelis Papakonstantinou

2013 – 290 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print)

ISBN 978-92-79-33275-3

doi: 10.2788/29861

Abstract

The objective of this report is to comprehensively inventory and analyse privacy and related certification schemes in the European Union and, where relevant, at the international level. The report will provide insights into the importance of privacy seal schemes and present information on the operational aspects of these schemes. The report will also help understand the privacy and data protection elements of the analysed schemes and provide an initial analysis of their shortcomings. The report specifically aims to understand whether (if at all) the analysed schemes address the requirements proposed under the GDPR. It will highlight the main convergences and differences between the schemes, who benefits from such schemes and what the impact of such schemes is.

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.



ISBN 978-92-79-33275-3



9 789279 332753