International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: http://www.tandfonline.com/loi/cirl20

The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR

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

To cite this article: Rowena Rodrigues, David Barnard-Wills, Paul De Hert & Vagelis Papakonstantinou (2016): The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2016.1189737

To link to this article: http://dx.doi.org/10.1080/13600869.2016.1189737

Published online: 28 Jun 2016.

International Review of Law, Computers & Technology, 2016
http://dx.doi.org/10.1080/13600869.2016.1189737

Routledge
Taylor & Francis Group

The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR

Rowena Rodrigues[a*], David Barnard-Wills[a], Paul De Hert[b,c] and Vagelis Papakonstantinou[c,d]

[a]*Trilateral Research Ltd., Crown House, 72 Hammersmith Road, London W14 8TH, UK;* [b]*TILT, Tilburg University, Tilburg, Netherlands;* [c]*Law Science Technology & Society (LSTS), Vrije Universiteit Brussel, Building B, room 4B317, Pleinlaan 2, B-1050 Brussels, Belgium;* [d]*PK partners Law Firm, Athens, Greece*

(*Received 10 November 2015; accepted 18 February 2016*)

The EU faces substantive legislative reform in data protection, specifically in the form of the General Data Protection Regulation (GDPR). One of the new elements in the GDPR is its call to establish data protection certification mechanisms, data protection seals and marks to help enhance transparency and compliance with the Regulation and allow data subjects to quickly assess the level of data protection of relevant products and services. To this effect, it is necessary to review privacy and data protection seals afresh and determine how data protection certification mechanisms, seals or marks might work given the role they will be called to play, particularly in Europe, in facilitating data protection. This article reviews the current state of play of privacy seals, the EU policy and regulatory thrusts for privacy and data protection certification, and the GDPR provisions on certification of the processing of personal data. The GDPR leaves substantial room for various options on data protection certification, which might play out in various ways, some of which are explored in this article.

Keywords: privacy seals; data protection seals; certification mechanisms

1. Introduction

Privacy seals schemes are voluntary privacy measures adopted as an industry self-regulatory initiative to promote consumer trust and confidence in e-commerce.[1] There is no fixed definition of a privacy or data protection seal, although a number of schemes in the market that offer some or the other form of certification based on privacy-related criteria, identify their offerings as privacy seals. A privacy seal is 'a certification mark or a guarantee issued by a certifying entity verifying an organisation's adherence to certain specified privacy standards that aim to promote consumer trust and confidence in e-commerce' (Rodrigues, Wright, and Wadhwa 2013). A privacy seal scheme might also certify the meeting of data protection criteria. Privacy seals are a visual way of representing that some third party believes a certified entity has met a particular set of standards or requirements. A privacy seal is a one-to-many communication strategy. A seal scheme is the organisational and administrative structure surrounding the seal, including the criteria for determining eligibility to display the seal. While they have largely developed as industry self-regulatory measures, in recent years, they are even being issued by data protection authorities in

*Corresponding author. Email: rowena.rodrigues@trilateralresearch.com

Europe, which potentially aligns them with other policy goals (Moulinos, Iliadis, and Tsoumas 2004).

Privacy seals have been subject to much discussion and debate (Cline 2003; Connolly 2008; Hammock 2011; LaRose and Rifon 2007; Moores 2005; Moores and Dhillon 2003; Rodrigues, Wright, and Wadhwa 2013; Stanaland, Lwin, and Miyazaki 2011). Some of this has been positive, while some of it has highlighted the limitations of privacy seals to provide privacy assurance.

The supposed benefits of privacy and data protection seal schemes are largely centred upon communicating adherence to particular principles, and doing so in a relatively low cost and voluntary manner. The problem privacy seals purport to solve for both data processors (often websites and other online services, e.g. cloud service providers) and service users, is that users cannot independently determine the data protection or privacy behaviour of the processors. Privacy policies are unread and written in legal jargon. The privacy seal demonstrates, rapidly, and without much effort to the users, that the certified entity's data protection practice meets certain standards to the satisfaction of the certifying body. The benefits of privacy seals may include: generation of privacy and data protection accountability and oversight; provision of privacy assurances (Connolly 2008); reduction in the regulatory and enforcement burden without compromising compliance; enhancement of trust and confidence (McKnight and Chervany 2001); reputational, competitive and market advantages to entities using them; boost to trade and commerce; generation of privacy awareness; assistance in proving fulfilment of privacy and data protection obligations; encouraging the implementation and maintenance of privacy protection measures; and presenting a quick and accessible means to determine and verify privacy and data protection commitments (European Commission 2012). For policy makers, they offer to support the development of the digital economy without a great deal of onerous intervention or enforcement.

As privacy seals are generally associated with self-regulation, this pushes questions of trust and confidence back from the certified entity to the seal issuer or administrator. If the criteria used for certification purposes are weak or ambiguous, then they will either not be trusted, or mistakenly trusted by relying parties. This makes privacy seals inherently problematic in themselves.

The EU is undergoing substantive legislative reform in data protection, specifically in the form of the General Data Protection Regulation (GDPR) (European Parliament and the Council of the European Union 2016). One of the new elements in the GDPR is its call to establish certification mechanisms, data protection seals and marks. To this effect it is necessary to review this topic afresh and determine how data protection seals might work given the new role they will be called to play, particularly in Europe, in enhancing and facilitating data protection. This article reviews the current state of play (Section 2), the EU policy and regulatory thrusts for data protection certification (Section 3) and the new GDPR provisions on certification of processing of personal data (Section 4). This article then explores and analyses four options possible within the new GDPR regime (while recognising that the GDPR leaves some room for other consequent options on certification, which might be filled out in various ways) (Section 5): encouraging and supporting compliance with the GDPR certification regime (option 1); accreditation of certification bodies (option 2); certification by national data protection authorities (option 3) or a mix of these options (option 4). One possible scenario envisaged in the GDPR is also the introduction of an EU data protection seal based on criteria approved by the European Data Protection Board, this scenario will be dealt with when discussing option 3 and we will return to it in the concluding section (Section 6). The research question underlying this article is what

are the possibilities and limitations of using privacy and/or data protection seals in this context. The article provides the reader with an understanding of the context, the GDPR policy landscape and the room for manoeuvre within it.

In this article, we use the term 'privacy seals' when we refer to existing schemes that are broader in scope and context and not solely focused on, or based on data protection criteria. When specifically discussing the GDPR, we use the term 'data protection seal'.

2. Review of the current state of play

Currently, there are a number of privacy (and data protection) seal schemes in operation. Notable amongst these are: Cloud Security Alliance,[2] CNIL label (2015), ePrivacyseal,[3] ESRB Privacy Online Certification,[4] EuroPriSe (European Privacy Seal) (EuroPriSe 2015), Gigya's SocialPrivacy Certification,[5] Market Research Society (MRS) Fair Data (Market Research Society 2015), PrivacyMark System,[6] Privo Privacy certified,[7] Smart Grid Privacy Seal,[8] TRUSTe,[9] Trustify-Me Privacy Certification Seal,[10] TÜV privacy seal[11] and so on.

The current privacy seals marketplace is defined by heterogeneity, and the level of variation amongst seals often impacts their effectiveness by introducing confusion amongst both users and entities seeking certification. Whilst there are a relatively small number of models that seal schemes follow, there is a large degree of variation in how the core models are implemented. Some privacy seal schemes are broad in coverage (i.e. cover a wide range of privacy and data protection criteria, or function as general trust marks, e.g. BBB Accredited Business Seal, Seriedad Online), others are more specific in nature, e.g. The Market Research Society's Fair Data, or the Commission nationale de l'informatique et des libertés (CNIL) Label 'audit de traitements', and cover the certification of specific technologies, or specific aspects of privacy and data protection. The schemes have either an international (e.g. TRUSTe), regional (EuroPriSe) or national scope (CNIL Label). They are issued by private companies, data protection authorities, non-profit organisations, industry bodies and certification organisations (with the number of certified entities per seal ranging from 300,000 to fewer than three). Costs vary depending on the scheme. The validity period of a seal varies (with one year being the most common). Revocation[12] of certification and seals is highly exceptional. While some of existing schemes have a complaints mechanism, others have none. These variations can have significant implications for the claims that a seal scheme is legitimately able to make. For example, a scheme with active investigation of complaints, revocation of seals and clear, accessible policies can make more justified claims about the practices of certified entities and the extent to which they can be trusted, that a scheme with weak assessment and enforcement mechanisms.

However, the current EU context of privacy and data protection seals falls short of achieving the potential benefits desired of them. A comparative study (Rodrigues et al. 2013a) of existing privacy seal schemes, found that a large number of existing schemes do not propose specific guarantees about the protection of personal data and the schemes that are more specifically focused on data protection (aligned with EU law) have reached a limited audience so far. Many of the schemes (being based outside the EU although available and visible within) do not cover international transfers of personal data. The privacy and data protection elements of existing schemes are variable and inconsistent. The regulatory and compliance standards underlying these schemes are a patchwork, either legal or industry-based or a combination (e.g. EU or national data protection law or issuer-set criteria).

There are several concerns in relation to existing schemes. Many seal issuers have too close a relationship with their subscribers, a relationship often driven by commercial profit. Some schemes have been accused of favouring their business members (Rhee and Ross 2010). Other concerns include: disregarding complaints, weak and inefficient privacy and data protection guarantees, inefficient evaluation and verification processes, prevalence of counterfeit seals, security flaws, inactive scheme elements (Connolly 2008) lack of enforcement (Clarke 2001), poorly accessible policies, lack of uptake, low interest (Databank Consulting 2004), high charges, blurring between similar schemes and user confusion in understanding what is being certified (European Commission 2007). As an example of the concerns surrounding existing schemes, in November 2014, TRUSTe (arguably the most globally recognised privacy seal scheme) agreed to settle US Federal Trade Commission (FTC) charges of consumer deception about its certification programme and practices. The FTC ordered that TRUSTe directly or indirectly not misrepresent, in any manner, expressly or by implication: (a) the steps it takes to evaluate, certify, review, or recertify a company's privacy practices; (b) the frequency with which it conducts any such evaluation, certification, review, or recertification of a company's privacy practices; (c) its corporate status and its independence; and (d) the extent to which the person or entity is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy programme sponsored by TRUSTe (Federal Trade Commission 2014). Privacy and data protection seals are, therefore, a heterogeneous field with recurrent issues surrounding their coverage, claims and validity, but at the same time bringing benefits to various stakeholders such as users of a seal and consumers. In short, they provide limited benefits to individuals and many entities that could be certified tend to avoid them, thus in turn reducing their benefits to policy makers and also to the economy.

3. EU policy and regulatory thrusts for privacy and data protection certification

EU policy, particularly since 2006, has positively affirmed the value of data protection certification, as evidenced repeatedly by the European Commission (European Commission 2006, 2007, 2010a, 2010b), the European Parliament (European Parliament 2010), and the Article 29 Data Protection Working Party (Article 29 Data Protection Working Party 2010).

In 2012, the European Commission proposed reform of the EU data protection law and set out a 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 or GDPR) (European Commission 2012). On 15 December 2015, post-completion of the 'trialogue' process, the European Parliament, Council and the Commission reached agreement on the EU data protection reforms package (originally proposed by the Commission in January 2012 to 'make Europe fit for the digital age') (European Commission 2015). On 8 April 2016, the Council adopted the General Data Protection Regulation (GDPR), and on 14 April 2016, the Regulation was adopted by the European Parliament. While the Regulation entered into force on 24 May 2016, it shall apply from 25 May 2018. This Regulation will replace the EU Data Protection Directive (Directive 95/46/EC) (European Parliament and the Council 1995). The Commission will work together with the Member States and the data protection authorities – the future European Data Protection Board (EDPB)[13] – to ensure a uniform application of the new rules (European Commission 2015). Amongst

other reforms, the GDPR seeks to encourage the establishment of certification mechanisms, data protection seals and marks to enhance transparency and compliance with the Regulation, and to allow data subjects to quickly assess the level of data protection of relevant products and services (Recital 100). In particular, Article 42 of the GDPR introduces the possibility of establishing certification mechanisms, data protection seals and marks. This Article and other related provisions will be explored further in the next section.

In policy terms, data protection seals are positioned amongst other attempts to increase consumer trust and confidence, and as a means to maximise the economic and social benefits of information technology. Seals are a potentially attractive policy approach because they are voluntary, administratively relatively lightweight, and offer benefits for positive conduct as opposed to enforcement against illegal actions.

Seals and certification have been deployed at the EU level in other contexts and areas, including network and information security (the ISO/IEC 15408 *Common Criteria* for Information Technology Security), general product compliance (the CE marking scheme), the environment (e.g. the EU Ecolabel, the Integrated Pollution Prevent and Control Certificate, the Green Dot scheme), entertainment (Pan European Game Information – PEGI), and food provenance (Protected Designation of Origin and Protected Geographical Indication), with some measure of success (Rodrigues et al. 2013b).

The EU Ecolabel scheme, in particular, merits a closer examination. It was launched in 1992 when the European Community decided to develop a Europe-wide voluntary environmental scheme that consumers could trust. The scheme has 44,711 products and services comprising 2031 licences (September 2015 reporting period). It covers a huge range of products and services, including all non-food and non-medical, and is recognised across Europe. There are a number of positive aspects of the Ecolabel that an EU data protection seal scheme could learn from. For instance, it has a relatively simple application process with discounts for SMEs, micro-enterprises and applicants from developing economies. Whilst overseen by the Commission, the EU Ecolabel process includes the involvement of a wide range of stakeholders, including industry primarily as members of the European Ecolabel Board. Because the scheme works at a European level, it goes beyond the pre-existing national ecolabels that are often only known within national borders. This also helps curtail the proliferation of environmental labelling schemes, and encourages higher environmental performance in all sectors for which environmental impact is a factor in consumer choice.

The EU Ecolabel is a widely known and well established scheme, the voluntary nature of which means that it is not threatening to industry, but can potentially be beneficial. The EU Ecolabel bears the greatest resemblance to existing privacy seal schemes. It is voluntary, carries relatively low costs, and confers the rights to display a seal, which presumably provides some benefits in a competitive marketplace. The key difference is the extent to which privacy issues act as a differentiator in the marketplace in the same way that environmental credentials might currently do, and that the Ecolabel is awarded to outstanding products within particular product categories. Additionally, most Ecolabel products will be purchased whereas many online services that use privacy seals may not free to the consumer (by deriving revenue from advertising). An important element of the scheme is the certification requirement that Ecolabel products have reduced ecological impact compared with other similar products in the marketplace. If this requirement is maintained over time, with the standard of ecological impact continuing to improve, this could have beneficial impacts across entire industrial sectors. The Ecolabel, therefore, acts as a policy instrument with a specific direction, rather than simply producing a better-informed version of the status quo. This tendency would be desirable in an EU data protection seal that was intended to improve privacy and data protection practices over time.

4. The GDPR provisions on certification

The aim of the GDPR is to reinforce data protection rights of individuals, facilitate the free flow of personal data in the digital single market and reduce administrative burden. This section highlights the GDPR provisions relating to certification based on the final agreed version (European Parliament and the Council of the European Union 2016).
Recital 100 states,

> In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

Article 42 on certification states,

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.
2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.
3. The certification shall be voluntary and available via a process that is transparent.
4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.
5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.
6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.
7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43 deals with the certification bodies. Article 43(1) states that without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 (tasks) and 58 (powers), certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2)[14] where necessary, issue and renew certification. Each Member State shall ensure that the certification bodies are accredited by: (a) the supervisory authority which is competent according to Article 55 or 56; (b) the national accreditation body named in accordance with Regulation (EC) 765/2008 of the European Parliament and the Council (European Parliament and the Council 2008) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority, which is competent pursuant to Article 55 (competence) or 56 (competence of the lead supervisory authority).

Article 43(2) deals with conditions for accreditation of certification bodies. To qualify a certification body must:

- have demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
- have undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority, which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;
- have established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- have demonstrated to the satisfaction of the competent supervisory authority that their tasks and duties do not result in a conflict of interests.

Article 43(3) provides that the accreditation of the certification bodies shall take place on the basis of criteria approved by the supervisory authority, which is competent according to Article 55 or 56 or, pursuant to Article 63, the European Data Protection Board. In case of an accreditation pursuant to point (b) of paragraph 1, these requirements complement those envisaged in Regulation 765/2008 (setting out the requirements for accreditation and market surveillance relating to the marketing of products) and the technical rules that describe the methods and procedures of the certification bodies. Article 43(6) specifies that these requirements and the criteria shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit these to the European Data Protection Board, which shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means.

Article 43(4) prescribes that the certification body (referred to in Paragraph 1 of the Article) shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with the Regulation. The accreditation is issued for a

maximum period of five years and may be renewed on the same conditions as long as the body meets the requirements. The certification body referred to in Article 43(1) shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification.

Article 43(7) states that the competent supervisory authority or the national accreditation body shall revoke the accreditation it granted to a certification body (referred to in Article 43(1)), if the conditions for accreditation are not, or no longer, met or where actions taken by a certification body infringe the Regulation.

Article 43(8) states that the Commission shall be empowered to adopt delegated acts in accordance with Article 92 (exercise of delegation), for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1). The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognise the certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

The GDPR, specifically, separately calls upon the supervisory authorities, in Article 57(1)(n) to encourage the establishment of data protection certification mechanisms, data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5). It also calls upon the European Data Protection Board in Article 70(1)(n) to encourage the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 (codes of conduct) and 42 (certification).

The EDPB, in its prescribed tasks is also called upon (on its own initiative or, where relevant, at the request of the Commission) in Article 70(1)(o) to carry out the accreditation of certification bodies and its periodic review pursuant to Article 43(6) and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7). The EDPB shall specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42 and provide the Commission with an opinion on the certification requirements referred to in Article 43(8).

5. Four options for implementation the new GDPR provisions

Under the new GDPR mandate, a range of options is available for implementing data protection certification. We present four options that are possible to meet the GDPR vision of certification mechanisms, data protection seals and marks encouraging transparency and compliance with the Regulation, in line with Recital 100. The options demonstrate the range of possibilities that the GDPR supports. The options are: (1) encouraging and supporting the GDPR certification regime; (2) accreditation of certification bodies (3) certification by national data protection authorities; (4) co-existence of the above three. For each of these options we provide a short outline, explore their applicability, risks and uncertainties, obstacles to implementation, and make a general evaluation of the option against the requirements of a successful data protection certification scheme and the GDPR. Each of the four options would have different impacts on stakeholders such as individuals, other relying parties or users, existing privacy certification schemes, certified entities or scheme subscribers, standardisation and certification bodies, industry, regulators and policymakers, and these are also identified.

5.1. *Encouraging and supporting compliance with the GDPR certification regime (option 1)*

This option envisages the European Commission using various soft measures to stimulate, promote and encourage compliance with the GDPR regime for certification and seals, but leaving all other areas such as criteria setting to national supervisory authorities, who would either develop their own certification criteria and schemes and/or accredit other certifiers as they see fit, with the bounds of Articles 42 and 43. The Commission's role would be to encourage and support national supervisory authorities in this regard, without additional institutional structures, and without further delegated acts. The aim would be to encourage data protection certification through non-binding measures, including setting objectives and creating guidelines, essentially focusing upon the 'mechanisms to promote' certification mechanisms. If the Commission adopted a leadership role in this field, then the EU could set objectives and monitor progress towards these. Alternatively, the Commission could act as a point of coordination for policy dialogue and information sharing relating to the national implementation of certification and seals. The Commission could be involved in setting collective objectives for national supervisory authorities, commissioning and producing regular reports and impact assessment to understand and communicate how the certification regime is developing, and facilitate peer-review, comparative benchmarking and mutual criticism as well as the sharing of best practice.

There are examples of soft law measures used by the Commission in the areas of state aid (Cini 2001), social policy (Jacobsson 2004; Trubek and Trubek 2005), telecommunications (Sabel and Zeitlin 2008) and other areas. Soft law with no binding force, such as rules of conduct, has played a practical role in European integration and these examples suggest that the use of soft or hard law change in response to specific issues and policy context.

The key risk of this approach would be the potential for a disharmonised and divergent approach to certification amongst the supervisory authorities of Member States. Even well-constructed soft guidance from the Commission or the EDPB may be interpreted in different ways in different Member States, including the extent to which they are followed. Even information and best practice sharing are unlikely to result in the transposition of an approach from one Member State to another. This would contribute to increased disharmony in of the privacy seals sector (noting that this is already characterised by high levels of heterogeneity). This option might find it difficult to achieve the goals of Recital 100 and the call for a harmonised approach at the European level. In addition, this option may restrict the potential for a harmonised European Data Protection Seal.

The reliance upon soft measures could leave unanswered a number of questions about the details of a certification scheme. Certification, as set out in the GDPR, is embryonic and would likely require further specification – for example about what is to be certified, and the criteria and requirements for certification. These questions are crucial, and could be, potentially problematic under this option. Whilst the Commission and the EDPB could produce guidance, this guidance and support could still be adopted or interpreted in different ways in different EU Member States. This option could find it difficult to resolve differences of opinion whilst still keeping the certification methods open. Similarly, the guidance and support would need to include a harmonised discussion on the desired policy objectives of the certification scheme, as well as the priorities that derive from this.

This option does risk some confusion between the role of the European Commission in facilitating coordination between different certification regimes and the potentially similar coordinating (and dispute resolution) role of the European Data Protection Board. The EDPB is empowered by the Regulation to establish data protection certification

mechanisms, seals and marks, and carry out the accreditation of certification bodies etc. The Commission is however able to bring more resources to the situation, and if the activities of the two bodies are themselves coordinated, then their efforts would be complementary. If the EDPB pursued the development of a coordinated European Data Protection Seal then this becomes more important.

This option potentially fails to address several gaps identified in the current landscape of privacy seals in the EU (De Hert et al. 2014). These include: lack of a warranted level of protection for personal data, lack of user awareness of schemes (Tschofenig et al. 2013), lack of user trust and confidence in schemes, lack of incentives for use and implementation of schemes (Tschofenig et al. 2013), deceptive potential of schemes, schemes justifying increased collection and use of personal data, enforcement issues, lack of regulatory oversight, lack of harmonisation and common standards, conflicts of interest and transitory nature of schemes. The certification elements in Article 42 of the GDPR, if undertaken by national supervisory authorities would address the lack of a warranted level of protection for personal data, lack of regulatory oversight, deceptive potential of schemes (by providing a non-deceptive option) and potentially the transitory nature of the schemes (the certifications are intended to be valid for three years under the GDPR, accreditation of certified bodies would be valid for five years). However, even if the Commission is able to encourage harmonisation between national efforts, issues are likely to remain in relation to the lack of incentives for the use and implementation of the scheme. Adding more data protection seal schemes in the EU is unlikely to eliminate concerns of fragmentation, duplication of efforts and waste of resources.

This option is a relatively lightweight and flexible option, dependent upon the type of support activities that are put in place. The GDPR appears to give criteria-setting authority to the Data Protection Authorities and this option conforms to this. The Commission can play a support role in this manner (e.g. as envisaged by the GDPR in laying down technical standards for certification mechanisms, and data protection seals to promote and recognise then), and has done so in the past. However, this option does risk limited and unevenly distributed effectiveness, with the potential for a lack of harmonised implementation of the GDPR certification regime. Whilst the option provides flexibility, and the option of scaling-up or moving from this option to one of the other following options if required, this option may not meet expectations for a European Data Protection Seal, have the success factors previously identified, and might fail to address existing gaps identified in relation to data protection seals.

5.1.1. *Impact on stakeholders*

This option may have a negative impact or maintain the status quo for individuals (i.e. it will not reduce the current heterogeneous landscape of privacy seals in the EU, with the associated problems of understanding the claims made by a particular scheme). Owing to the limited harmonisation potential of this option, it could result in information costs (for organisations that rely on privacy certification) to find a scheme that offers adequate certification. Existing privacy and data protection seal schemes, especially European ones, could experience a growth in the number of their competitors as new private accredited schemes emerge and Member State supervisory authorities launch or advance their own certification schemes.

Scheme subscribers will be burdened with seeking certification through different schemes in different Member States. Data controllers and processors would have to determine where it is appropriate to seek certification and certification requirements could be

quite divergent in different jurisdictions (although they would all be based upon the core requirements of the GDPR). Certified entities may thus be able to engage in forum shopping to find certification processes with easier requirements; thus there is a potential for divergence and for less harmonised certification regimes to develop in Member States. Incompatible regimes would increase the burden on data controllers and processors operating in multiple Member States and seeking certification.

The soft measures and coordination activities may contribute towards harmonisation of data protection certification in the EU, but the diversity of implementation that is likely to result from this option will affect that. A lack of harmonisation under this approach could increase the difficulty and complexity of non-EU entities attempting to bring services to the EU market in understanding the requirements of certification, and the extent to which certification obtained in one Member State is applicable in others.

5.2. *Accreditation of certification bodies (option 2)*

The GDPR sets out three possibilities regarding the accreditation of certification bodies: one, accreditation by the national supervisory authorities, the second, accreditation by the national accreditation bodies and the third, accreditation of certification bodies by the EDPB. The GDPR provides preliminary conditions for the accreditation of a certification body. A certification body may be accredited only if:

- it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
- it has undertaken to respect the criteria approved by the supervisory authority or the European Data Protection Board;
- it has established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;
- it has demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

5.2.1. *Accreditation by national supervisory authorities*

Under the GDPR, national supervisory authorities have the power to accredit certification bodies pursuant to Article 43(1)(a) (subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law) and to draft and publish the criteria for accreditation of a certification body pursuant to Article 43(3).

The UK Information Commissioner's Office (ICO) announced a co-regulatory approach to privacy seals (Information Commissioner's Office 2015a). The ICO expects to 'endorse third party operators to deliver ICO privacy seal schemes. Once approved, the scheme operators will be responsible for the day-to-day running of the scheme' (Information Commissioner's Office 2015b). The ICO anticipates different scheme operators will focus on different sectors, processes, products or areas of compliance. It further suggests that potential scheme operators must be accredited by the UK Accreditation Service (UKAS) and will need to meet a 'strict set of criteria' developed by its office. The criteria aims to 'ensure that any ICO privacy seal scheme is viable, promotes the high standards' and 'complements the existing priorities' of the ICO. The ICO would retain the right to

remove its endorsement if the operator is no longer able to run the scheme to the required standard. As of the end August 2015, the ICO suggests its 'privacy seal should be up and running before that Regulation comes into force'.[15] A 2014 report presenting topline findings from the ICO's Annual Track 2014, which measures awareness of the Data Protection Act (DPA) and Freedom of Information Act (FOIA) amongst the general public, states that

> There is widespread support for the introduction of a new certification mark to show that an online service provider has been accredited in protecting information rights, with four in five of the respondents (81%) say they approve, with 44% strongly approving (ICO 2014).

Existing privacy seal schemes have various shortcomings and are not up to the level envisaged in the GDPR. Some of these schemes might find it beneficial to revise their certification criteria and requirements to bring these in line with conditions set by the GDPR. Here, the schemes would have a chance to fulfil their desire to meet such criteria and bring further advantage to themselves, as being compliant with the Regulation.

5.2.2. *Accreditation by NABs*

The GDPR, in Article 43(1)(b) states that certification bodies might also be accredited by the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012 (International Organization for Standardization 2012) and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56 of the GDPR. In case of such accreditation, the GDPR requirements complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

5.2.3. *Accreditation by the EDPB*

According to Article 70(1)(o) of the GDPR, the European Data Protection Board, on its own initiative or, where relevant, at the request of European the Commission, shall: carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6), and of the accredited controllers or processors established in third countries pursuant to Article 42(7). The Board may, specify the requirements for the accreditation of certification bodies under Article 43.

Existing privacy certification schemes could apply for accreditation and if found compliant with the set criteria and requirements, would be certified. Non-EU based schemes could also apply for accreditation (the GDPR does not exclude them and this is important given its vision for demonstrating that controllers and processors outside the EU and not subject to the GDPR's jurisdiction have appropriate data protection safeguards).

The intent seems to be to promote harmonisation across the EU, to address the heterogeneity in the differential requirements and criteria of existing privacy certification schemes, facilitate consistency in their offerings and practices, improve the quality of existing certification schemes, and foster trust and confidence in them. Existing schemes could thus be a part of an EU umbrella framework for data protection certification.

One of the biggest problems of the existing privacy seals scenario is that current schemes operate in a largely self-regulatory, fragmented environment. There is no way for an individual or relying party to decide which scheme to trust the most (or even trust at all). The possibilities of accreditation supported by the GDPR help eliminate this

problem by providing existing privacy and data protection seal schemes with a framework against which to evaluate their offerings and bring their practices in line with EU requirements, standards, and societal expectations, which can then percolate down through the privacy certification chain to the final relying party.

This option has the potential to leverage existing resources (i.e. the competencies of the supervisory authorities and the NABs), but also implies significant additional resource burdens (costs and human) particularly for the supervisory authorities and the European Data Protection Board. The EDPB, in particular, would require adequate resources, and certification and accreditation expertise. It would need to actively monitor and oversee the accreditation mechanisms across the EU and conduct market surveillance to ensure that the accreditation is not misused in any manner. This is why it is important that the EDPB collect information on accredited certification bodies (and document instances of revocation) and make it publicly available through appropriate means. What is not clear is how the power of the EDPB to set the criteria would be reconciled with its power to accredit certification bodies; we think separation of the criteria-setting body and the accreditation body is important to ensure that there is no bending of rules or compromise of the underlying objectives of the accreditation.

The register should be an authoritative source of information on all the approved certification schemes, seals, and marks. It would be updated as often as required when changes occur, and should include information on privacy certification schemes that have been removed from the register. It would enable the public to know whether a particular privacy certification scheme met the EU standards or not. It would also help applicants decide whether they should subscribe to schemes that are not listed on it. A similar model can be found in the European Network and Information Security Agency's (ENISA) Cloud Certification Schemes List (ENISA 2015) which collates available certification schemes for cloud computing and shows their main characteristics, including their underlying standards, audit regimes and other relevant factors. That list does not, however, formally accredit the cloud certification schemes, rather it provides information on them in a comparable manner.

The GDPR framework for certification is primarily voluntary and dependent on the course of action adopted by the Commission, EDPB and the national Member States. Further, unless there are legal, economic or competitive advantages, privacy certification schemes might not see value in applying for accreditation. Further, it is not clear whether existing privacy seal schemes would be willing to open themselves, their criteria, processes and procedures to this scrutiny. How this could be boosted, i.e. how certification bodies might be encouraged to become accredited, could benefit from further research.

There is currently no scheme that accredits privacy certification schemes at the EU level to pre-defined EU criteria and requirements. While certification might be viewed often as a purely commercial activity, the accreditation possibilities examined here, are not of that nature. However, they should be carefully exercised. Their ultimate success will depend on whether it brings added value, is sustainable in the long run and helps generate more confidence and trust in data protection certification (mechanisms, tools and scheme operators).

5.2.4. *Impact on stakeholders*

Accreditation of certification bodies presents individuals with a better means of assessing certification schemes with greater confidence; something that is still not sufficiently within their reach. It would help individuals decide and discern which schemes to trust.

Relying parties and users of existing schemes might demand that such schemes get accredited in line with the GDPR. They will also have better assurance about the claims being made, especially in cross-border contexts.

Accreditation has resource burdens for those that apply for accreditation. This might mean that only schemes that can devote time or other resources (e.g. financial, human), and are open to the idea of being accredited, will apply. However, the GDPR does provide a soft incentive for schemes to apply for accreditation.

Accredited certification schemes might gain a competitive and, more importantly, reputational advantage over non-accredited certification schemes – in turn, they may be able to use their accredited status to draw in a greater number of applicants, not only from their country of establishment but also across Europe and even outside Europe. Depending on the scope of the accreditation, non-EU based schemes could also apply for certification and gain market and reputational advantages. Non-accredited schemes might lose business and profits as applicants decide to go with schemes that have been approved under this option and listed on the register.

Certified entities (scheme subscribers) will be able to have greater confidence and trust that the scheme they are applying to, has been accredited and meets the set EU standards and requirements, rather than just being based on arbitrary or misaligned criteria. Thus, they may show greater willingness to apply and continue to remain a part of schemes that have been accredited by DPAs, NABs or the EDPB. This will help address the gaps identified in the privacy seals sector and help schemes to grow.

Further, in enabling schemes to open up their criteria and practices and in harmonising the EU-level criteria, this will facilitate and improve privacy and data protection, efficiency and boost the image of data protection certification mechanisms, seals and marks. This is in tune with the goals of the Internal Market and will strengthen the competitiveness of European privacy and data protection certification schemes, and create desirable conditions for their economic growth, although questions of subsidiarity may arise in relation to whether an EU-wide privacy seal scheme could be achieved without a centralistic approach.

The possibilities explored in this section will require new EU and national-level policy and legislative measures and there will be an administrative impact in terms of costs. However, this will demonstrate leadership from the EU in harmonising its privacy and data protection certification sector. The possibilities might also present benefits to international consumers who rely only on seals that are registered in the (EU) register.

5.3. *Certification by national data protection authorities (option 3)*

The GDPR, Article 42(5) states that a competent supervisory authority may issue certification on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. This option envisages that the certification itself would be run by Member State data protection authorities (DPAs). The DPAs would therefore be involved in this process directly, by certifying applicants as in case of the French CNIL Label.

National DPAs would run the scheme, applying criteria either approved by themselves or by the European Data Protection Board. In the event of criteria set by the Board, while these would need to be both detailed enough and enforceable at Member State level to avoid diverging schemes and reproduction of the fragmentation evident in existing EU privacy seal schemes, DPAs could still be left with substantial space for operational flexibility

while implementing the scheme at the national level. Evidently, in the event of criteria set by the DPAs themselves, such an operational flexibility level would be substantially increased, allowing for diverging approaches on this issue among Member States or even, ultimately, intra-EU competition among such schemes.

Regardless of the specific method through which the criteria list will be devised, it will have to address a number of important issues varying from strategic and planning matters (for instance, whether the scheme will have an EU logo, whether it shall be sector-specific or cross-sector, whether it will certify products and/or services and/or processes, the scheme's financial details, etc.) to actual implementation details (e.g. the legal status of the seal at Member State level, the redress mechanism available to data subjects, data controller obligations with regard to the scheme, the level of flexibility afforded to Member State DPAs, etc.). All of these entail important decisions that will determine, in essence, the nature of the seal scheme as a whole. In the same context, because monitoring and updating of the scheme are central elements of a successful certification scheme (De Hert et al. 2014), either the Board or the DPA setting the criteria and requirements would need to be involved in these tasks. This, however, involves substantial commitment and involvement in frequently sector-specific and detailed personal data processing operations.

At the Member State level, the risks refer mostly to the DPAs' perceived role and actual capacity to perform their tasks under this policy option. With regard to the former, DPAs are customarily viewed as independent regulators of data controllers and provide assistance to data subjects in exercising their rights, and they are supported in this by applicable legislation. Their actual and perceived independence is, therefore, essential in the execution of their duties. Their potential involvement in directly awarding data protection seals to data controllers (presumably, for a fee, even if nominal) risks a conflict of interest with regard to their mission, because they will be at the same time regulators and certifiers (a 'function creep' effect). Difficulties might arise in cases where a DPA might have to penalise a data controller, certified by it, for its personal data processing. It is therefore important for DPAs to safeguard their role in the EU data protection system, a task that could be compromised by their simultaneous role as data protection certifiers.

Under the data protection system in effect today in the EU, DPAs are independent authorities that monitor the application of, and ensure respect for, data protection legislation within their territories. If Member State DPAs choose to award privacy or data protection seals directly to data controllers, they run the risk that, despite their best intentions and efforts, they will be viewed as having conflicting interests in the process. In practice, it will be difficult to imagine a data controller that carries a seal awarded by a DPA to be independently regulated at a later stage by it (and even found guilty of data protection infringement). In such a case, even under the best circumstances of transparency and rule of law, data subjects might view the dual role of DPAs with suspicion. This might lead to a loss of public trust, an otherwise critical element for the success of a privacy or data protection seal scheme (De Hert et al. 2014).

Similarly, the operation of a privacy or data protection seal scheme directly by DPAs could test their, already burdened, capacity. The recent exponential growth of personal data processing, and therefore of DPA involvement in controlling it, has added to their workload (European Union Agency for Fundamental Rights 2010). The operation of a complete seal scheme that would require a permanent mechanism with provisions for evaluations to back office support, would add substantially to their tasks. It is possible that certain DPAs of smaller EU Member States are not in possession of the expertise or sufficient resources to run such a scheme successfully. There are, of course, instances of DPAs

running privacy seal schemes. For instance, the French Commission Nationale de l'Informatique et des Libertés' (CNIL) scheme (CNIL Label) that certifies compliance with the French data protection law ('Labels CNIL'). The Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), the Office of the Data Protection Commissioner of Schleswig-Holstein, Germany certifies compliance of hardware, software, automated procedures and services with German/Schleswig-Holstein data protection law (Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein 2015). However, their uptake is limited.

A further substantial obstacle for the adoption of this policy model relates to the requirement for extensive regulatory (or, at least, institutional) intervention prior to its launch. As described above, the first stage of implementation would involve important decision-making either at the EU (Board) level or at DPA (Member State) level. This involves option selection, detailed elaboration and setting of the common criteria and requirements for the establishment and operation of the certification and accreditation schemes. This process will be time-consuming, regardless of whether undertaken by the EDPB (with ensuing coordination and cooperation issues) or by a DPA. In the event of a European Data Protection Seal, once concluded, the same process will need to take place at Member State level: depending on the level of flexibility permitted to DPAs, a series of important decisions will need to be made with regard to the actual operational model they will implement. Such decisions will evidently need to be incorporated into formal documents (ranging from legislative acts to contracts). Only after all of the above are concluded, could the data protection seal scheme be launched.

5.3.1. *Impact on stakeholders*

Under this option, the protection afforded to individuals will be high due to the involvement of the DPAs. However, the aforementioned risk of a, presumed or true, conflict of interest must not be forgotten. The implementation of any EU data protection seal scheme seeks to achieve an increased level of trust and confidence, as per its declared objectives. It is perceived that the ultimate level of public trust and confidence vested in certified organisations, products and services, although already high given DPA involvement, will vary depending on the actual model implemented within each Member State. If DPAs assume directly the role of certifiers, the underlying conflict of interest might adversely affect public trust and confidence in the overall scheme.

Under this option, existing privacy certification schemes would continue to operate as usual. This would admittedly offer them the possibility to expand and further their scope. However, the issue of competition among EU data protection Member State certification schemes also ought to be addressed: in the event, for instance, the one Member State scheme was made available to all EU data controllers while other DPA-seals coexisted with it at Member State level, an undesirable competition among schemes could be created. There is also the issue that private privacy certification schemes would face competition from the DPA-run schemes. The former would face a disadvantage as their services and offerings might be seen to be less trustworthy and compliant and they might face the danger of losing business and becoming obsolete.

From the scheme subscribers' or certified entities' perspective, any successful EU data protection seal scheme could enhance their market reputation and credibility, create legal certainty and enhance the maturity of their data protection management systems. EU standardisation bodies might have an (indirect) role to play in this option, if they contribute to a harmonised European standard or family of standards for data protection certification

schemes through the European standardisation (EN) framework that would have to be later incorporated into formal DPA or Board criteria, or they are involved as relevant stakeholders in an EU level consultation on the criteria and requirements for the scheme.

Any data protection seal programme would benefit the industry that chooses to have its members certified, due to increased public trust, enhanced reputation, and enhanced maturity of data protection management systems. This is particularly true for this policy option due to the DPA involvement in the scheme.

While the involvement of DPAs, directly or indirectly, in the scheme's operation would guarantee an increased level of protection for individuals and a series of benefits for certified entities, Member State implementations could vary considerably and raise practical questions as regards mutual recognition of the various seals under the certification programme. In particular, it should also be decided whether a potential European Data Protection Seal would be exclusive of other DPA-run seals. If this happens, the harmonisation effect that constitutes an important priority for an EU data protection seals scheme would probably not be achieved: multiple implementations could lead to data subject uncertainty and data controller forum shopping. In addition, the strategic decisions that would need to be taken at the EU level could equally assist or hinder harmonisation among Member States even further: issues such as the seals scheme branding (a common EU logo or not), the level of detail in the common EU criteria and requirements and whether the scheme will operate at multi- or single-processing sector level constitute important decisions that would need to strike the balance between guaranteeing flexibility and ensuring a level of harmonisation and integration among Member States.

An EU data protection seal scheme would facilitate the exercise of data protection rights by data subjects, and create increased legal certainty for data controllers. The involvement of Member State DPAs in the scheme, regardless of their exact role, warrants a possibly higher level of attaining those objectives, while at the same time benefiting European society.

Regulators and policy makers might be involved under this policy option at two stages: first, in drafting the common criteria for the EU data protection seal scheme and, subsequently, at Member State level, in making the scheme concrete to local choices and peculiarities. Once implemented within national borders, a number of other mechanisms will presumably be involved in enforcing the scheme (DPAs, courts), furthering it (state bodies, industry associations, standard-setting organisations) and making it sustainable (state and other resources). At each stage, there is a need for coordinated actions and informed choices that would benefit not only broader data protection purposes, but also result in an effective and sustainable EU data protection seal scheme.

Given the multitude of strategic planning choices that need to be made at the EU and Member State level under this policy option, it is difficult to currently foresee the international impact this option would have on the wider international community. It is only after the central, EU-wide decisions have been made and the system becomes operational in a significant number of Member States, that its performance will decide whether it will constitute an exportable element of the EU data protection model.

5.4. *Coexistence of the above three (option 4)*

The first option would coexist with, and support both the second and third options. The EDPB, as a point of contact between data protection authorities, would be an important part of any soft-law or best practice sharing approach. The sharing of best practice,

providing guidance and exemplar models would be most useful in the third option, where this can potentially help to counter the risk of de-harmonisation. DPAs in the EU are in regular contact, and share best practice on many aspects of their work (Barnard-Wills and Wright 2015) and could be expected to do so with regard to certification. Option 2 Accreditation of certifiers and Option 3 Certification by national data protection authorities are intricately connected, as envisioned by the GDPR. Certification in line with Article 42 of the GDPR can only be issued by duly accredited bodies or by the competent supervisory authority, on the basis of the criteria approved by that authority or by the EDPB. Article 42(5) also clarifies that in the latter case, the criteria approved by the European Data Protection Board may result in a common certification, the European Data Protection Seal.

Table 1 presents the pros (+) and cons (-) of the four options.

Table 1. Four options and their pros and cons.

Encouraging and supporting compliance with the GDPR certification regime
+ Successfully used in other areas such as social policy, state aid, etc.
+ Flexibility; room for manoeuvre according to national needs, policy etc.
+ Initiatives by national DPAs fit well here
+ Might be better placed to address issues of technological innovation
– Light touch approach might not be the best to achieve GDPR vision
– Potential for a disharmonised and divergent approach to certification
– Misinterpretation, application of guidance
– Could leave unanswered a number of questions
– Fails to address several gaps identified in the current landscape of privacy seals in the EU
Accreditation of certifiers
+ Harmonisation in EU privacy certification schemes
+ Facilitates consistency in their offerings and practices across the EU
+ Improves the quality of existing certification schemes and fosters trust and confidence in them
+ Value added for non-EU based schemes
+ Permits existing schemes to continue to exist under an EU umbrella
+ Provides an individual or relying party with the parameters of trusting schemes
– Resource particularly cost burdens
– Unless there are legal, economic or competitive advantages, schemes may not see value in applying for accreditation
– Existing schemes might not be willing to open themselves up to scrutiny
– Power to EDPB to set accreditation criteria and accredit certifiers (role conflicts)
Certification by national data protection authorities
+ Direct involvement of DPAs
+ More reliable, criteria underlying schemes
+ Would generate greater trust and confidence in schemes certified by the DPA, EDPB
+ Greater protection and protection assurances for individuals' personal data
– Risk in relation to the perceived role of the DPA (function creep and conflict of interest)
– Questions about the impartiality of DPA as regulator depending on type of scheme and separation of powers
– Risk of the 'DPA certified' and 'certified-nots'
– Need to harness DPAs resources and actual capacity to perform their tasks under this policy option
– Requirement of extensive regulatory (or, at least, institutional) intervention prior to its launch
Coexistence of the above three
+ Coordination efforts may limit proliferation of seal types
– Potential for incompatibility between accreditation of certifiers by EDPB and by national data protection authorities.

6. Looking to the future: a harmonised European data protection seal?

This article has examined the current landscape of privacy seals and their limitations, examined the policy drive for EU privacy seals coming from the data protection reform processes as manifested in the GDPR, and evaluated four ways in which this might conceivably play out. It has argued that seals still have significant issues, but the potential in certain areas for certain types of data protection, risk communication and assurance problems. The article demonstrates that if data protection and privacy seals are to be supported in policy, this must be done carefully and with reference to these limitations and to past experiences (negative and positive) with seals in other contexts.

In addition to having different impacts upon stakeholders and offering different approaches to meeting the requirements of the GDPR, the four options presented in this article highlight several remaining issues with the deployment of EU data protection certification mechanisms, seals and marks. Several seal-based options are available that appear to meet the requirements of the GDPR.

A key issue is the ambiguity of the role of DPAs in certification, and the relationship of this to their enforcement role. Shared criteria and mechanisms for certification across DPAs, and a clear and consistent role for the EDPB will be increasingly important in this field. One clear lesson emerging from this analysis is the requirement for DPAs to exercise careful organisation and coordination amongst themselves on this issue. The GDPR provisions still leave open the efficacy of data protection seals in providing any competitive advantage to certified parties. It also leaves open the efficacy of seals for actually improving data protection practice (companies with good policy and stronger incentive to will seek certification, those without will not). This is particularly exacerbated by the ease with which privacy can be violated across contexts and domains. Little in the policy options available under the GDPR addresses the core heterogeneity (and limited quality) of the existing privacy and data protection seals market. The possibility of using one or more options might itself result in a further proliferation of seals in Member States and also might not help address the need for cross-border applicability.

The active development of data protection seals by DPAs prior to the GDPR may affect (or at the very least inform) the way that the post-GDPR certification regime comes about. 'Seals' by themselves, although they may go some way to achieving a certain level of data protection assurance, will only be as good as the scheme underlying it.

The new GDPR in fact leaves substantial space for decision-making. In particular, its provisions allow anything from maintenance of the current (limited) model of DPA-run seals, to the accreditation of certification, and even to the creation of a European Data Protection Seal. However, each one of these models requires careful planning and coordination in order to profit from its advantages and possibly avoid the inevitable, problematic issues. An entirely DPA-run scheme would overstretch DPAs' already limited resources, even lead to a 'function creep' effect. The relationship among several, simultaneously operated and ultimately competitive DPA-run seals' schemes in the EU ought to also be clarified in order to avoid unwanted competition among them.

A European Data Protection Seal may appear an appealing option for harmonisation purposes but it includes substantial coordination and cooperation among Member States. In addition, a decision needs to be made about whether its existence would be exclusive to any other DPA-run schemes in the EU, or whether it would be solely an exportable seal (addressed to non-EU entities). All of the above require careful planning and analysis. On the other hand, current purely private sector, and unrelated to any DPA, initiatives are most likely not compatible with the new GDPR provisions and will probably

have to take advantage of the two-year period until its coming into effect in order to re-adapt.

The four options presented in this article each have their pros and cons. We have to underline that what is important is that the EU data protection seal scheme takes into account the lessons learnt from the past experience of privacy seals. If an EU data protection seal is to bring real value, it must be a robust and strong data protection mechanism to give data subjects' true (and not just symbolic) reassurance about the protection of their personal data. The more robust the data protection criteria and the process of certification, the more effective the EU data protection seal will be. By itself, a European data protection seal might not be the strongest means of enhancing transparency and compliance with the GDPR, and there are real limitations to what seals can achieve, but if well-implemented, data protection certification mechanisms and seals might go some way to helping EU data subjects quickly assess the level of data protection of relevant products and services.

Acknowledgement

This work draws inspiration from the research and results of the EU Privacy Seals Project commissioned by the European Commission, 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), Service Contract Number 258065. The views in this article are those of the authors alone and are in no way intended to reflect those of the European Commission.

Conflict of Interest Disclosure

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by European Commission, 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): [Grant Number Service Contract Number 258065].

Notes

1. The European Commission recognises the need to improve consumer confidence in cross-border shopping online by taking appropriate policy action. According to the European Commission, 'empowered and confident consumers can drive forward the European economy'. 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.
2. https://cloudsecurityalliance.org/star/
3. https://www.eprivacy.eu/en/privacy-seals/eprivacyseal/
4. http://www.esrb.org/privacy/
5. http://www.gigya.com/blog/announcing-gigya-socialprivacy-certification-and-new-consumer-privacy-survey-results/
6. http://privacymark.org/
7. https://privo.com/
8. https://www.truste.com/business-products/trusted-smart-grid/
9. https://www.truste.com/business-products/dpm-services/#pCert
10. http://trustifyme.org/
11. https://www.tuvit.de/en/privacy/uld-privacy-seal-1075.htm

12. Grounds might include failure to allow access or inspection, violation of terms of agreement, failure to properly display seal, violation of any law on the part of the certified entity (as determined by the seal authority), failure to correct issues raised by seal authority etc.
13. According to Recital 139, GDPR, the EDPB should be set up as an independent body of the Union with legal personality and would be represented by its Chair. It would replace the Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It would consist of a head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The EDPB would contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. It would act independently when exercising its tasks.
14. Corrective power of the supervisory authority to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Article 39 and 39a, or to order the certification body not to issue certification if the requirements for the certification are not or no longer met.
15. https://iconewsblog.wordpress.com/2015/08/28/whats-the-latest-on-the-ico-privacy-seals/

References

Article 29 Data Protection Working Party. 2010. "Opinion 3/2010 on the Principle of Accountability, WP 173." Adopted on 13 July 2010.

Barnard-Wills, David, and David Wright. 2015. *Authorities Views on the Impact of the Data Protection Framework Reform on their Cooperation in the EU*. London. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA2_D1_20150720.pdf.

Cini, M. 2001. "The Soft Law Approach: Commission Rule-Making in the EU's State Aid Regime." *Journal of European Public Policy* 8 (2): 192–207.

Clarke, Roger. 2001. "Meta-Brands." *Privacy Law and Policy Reporter* 7 (9). Accessed November 1, 2015. http://www.rogerclarke.com/DV/MetaBrands.html.

Cline, J. 2003. "Web Site Privacy Seals: Are they Worth It?." *Computerworld*. May 8. http://www.computerworld.com/s/article/81041/Web_site_privacy_seals_Are_they_worth_it

Commission nationale de l'informatique et des libertés (CNIL). 2015. "Labels CNIL." Accessed November 1, 2015. http://www.cnil.fr/linstitution/labels-cnil/.

Connolly, C. 2008. "Trustmark Schemes Struggle to Protect Privacy 2008." Galexia, Version 1.0, September 26. http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/.

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

De Hert, Paul, Vagelis Papakonstantinou, Rowena Rodrigues, David Barnard-Wills, David Wright, Luca Remotti, and Tonia Damvakeraki. 2014. *Task 3 Challenges and Possible Scope of an EU Privacy Seal Scheme, Final Report Study Deliverable 3.4*. EU Privacy Seals Project Commissioned by the European Commission. Luxembourg: Publications Office of the European Union. http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26699/.

ENISA (European Network and Information Security Agency). 2015. "Cloud Computing Certification." Accessed November 1 2015. https://resilience.enisa.europa.eu/cloud-computing-certification.

European Commission. 2006. "Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A strategy for a Secure Information Society – 'Dialogue, Partnership and Empowerment'." COM (2006) 251. Brussels. May 31. http://ec.europa.eu/information_society/doc/com2006251.pdf.

European Commission. 2007. "Communication to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)." COM (2007) 228 final. Brussels, May 2.

European Commission. 2010a. *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*. Final Report. January 20. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

European Commission. 2010b. "Communication 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. November 4. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.
European Commission. 2012. "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. 25.01.2012.
European Commission. 2015. "Agreement on the Commission's EU Data Protection Reform will boost Digital Single Market." Press release. 15 December 2015. http://europa.eu/rapid/press-release_IP-15-6321_en.htm.
European Parliament. 2010. "Resolution of 15 December 2010 on the Impact of Advertising on Consumer Behaviour. 2010/2052 (INI)." http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0484+0+DOC+XML+V0//EN&language=EN.
European Parliament and the Council. 1995. "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. November 23: 31–50.
European Parliament and the Council. 2008. "Regulation (EC) No 765/2008 of 9 July 2008 Setting out the Requirements for Accreditation and Market Surveillance Relating to the Marketing of Products and Repealing Regulation (EEC) No 339/93." Official Journal of the European Union L 218/30 EN 13.8.2008.
European Parliament and the Council of the European Union. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)." *Official Journal of the European Union L 119* 59: 1–88. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
European Union Agency for Fundamental Rights. 2010. *Data Protection in the European Union: The Role of National Data Protection Authorities: Strengthening the Fundamental Rights Architecture in the EU II*. Luxembourg: Publications Office of the European Union.
EuroPriSe. 2015. "EuroPriSe – the European Privacy Seal for IT Products and IT-Based Services." Accessed November 1, 2015. https://www.european-privacy-seal.eu/EPS-en/Home.
Federal Trade Commission. 2014. *In the Matter of True Ultimate Standards Everywhere, Inc.*, a corporation. Agreement containing consent order. 2014. http://www.ftc.gov/system/files/documents/cases/141117trusteagree.pdf.
Hammock, M. R. 2011. "Do Certification Seals Permit a Price Premium for Online Security and Privacy?" *Policy & Internet* 3 (2). http://www.psocommons.org/policyandinternet/vol3/iss2/art7.
Information Commissioner's Office. 2014. Annual Track 2014. Individuals (Topline findings). September 20. https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf.
Information Commissioner's Office. 2015a. "Privacy Seals." Accessed November 1, 2015. https://ico.org.uk/for-organisations/improve-your-practices/privacy-seals/.
Information Commissioner's Office. 2015b. "What you need to know about ICO Privacy Seals." *Information Commissioner's Office Blog*, January 28. https://iconewsblog.wordpress.com/2015/01/28/what-you-need-to-know-about-ico-privacy-seals/.
International Organization for Standardization. 2012. "ISO/IEC 17065:2012: Conformity Assessment – Requirements for Bodies Certifying Products, Processes and Services." http://www.iso.org/iso/catalogue_detail.htm?csnumber=46568.
Jacobsson, K. 2004. "Beyond Deliberation and Discipline: Soft Governance in the EU Employment Policy." In *Soft Law in Governance and Regulation: An Interdisciplinary Analysis*, edited by Ulrika Morth, 81–101. Cheltenham: Edward Elgar Publishing.
LaRose, R., and N. J. Rifon. 2007. "Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior." *Journal of Consumer Affairs* Summer 2007 41: 127–149.
Market Research Society. 2015. "Fair Data." Accessed November 1, 2015. http://www.fairdata.org.uk/.
McKnight, D. Harrison, and Norman L. Chervany. 2001. "What Trust Means in E-commerce Customer Relationships: An Interdisciplinary Conceptual Typology." *International Journal of Electronic commerce* 6 (2): 35–59.

Moores, T. 2005. "Do Consumers Understand the Role of Privacy Seals in E-commerce?" *Communications of the ACM* March 48 (3): 86–91.

Moores, T., and G. Dhillon. 2003. "Do Privacy Seals in E-commerce Really Work?" *Communications of the ACM – Mobile Computing Opportunities and Challenges* 46 (12): 265–271.

Moulinos, K., J. Iliadis, and V. Tsoumas. 2004. "Toward Secure Sealing of Privacy Policies." *Information Management & Computer Security* 12 (4): 350–361.

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

Rodrigues, Rowena, David Barnard-Wills, David Wright, Paul de Hert, and Vagelis Papakonstantinou. 2013a. *Inventory and Analysis of Privacy Certification Schemes: Final Report Study Deliverable 1.4*, EU Privacy Seals Project Commissioned by the European Commission. Luxembourg: Publications Office of the European Union.

Rodrigues, Rowena, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki, Paul De Hert, and Vagelis Papakonstantinou. 2013b. *Comparison with other EU Certification Schemes, Final Report Study Deliverable 2.4*. EU Privacy Seals Project Commissioned by the European Commission Publications. Luxembourg: Office of the European Union. http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26700/.

Rodrigues, Rowena, David Wright, and Kush Wadhwa. 2013. "Developing a Privacy Seal Scheme (That Works)." *International Data Privacy Law* 3 (2). doi:10.1093/idpl/ips037.

Sabel, C. F., and J. Zeitlin. 2008. "Learning from Difference: The New Architecture of Experimentalist Governance in the EU." *European Law Journal* 14 (14): 271–327.

Stanaland, Andrea J., May O. Lwin, and Anthony Miyazaki. 2011. "Online Privacy Trustmarks: Enhancing the Perceived Ethics of Digital Advertising." *Journal of Advertising Research* 51 (3): 511–523.

Trubek, David M., and Louise G. Trubek. 2005. "Hard and Soft Law in the Construction of Social Europe: The Role of the Open Method of Coordination." *European Law Journal* 11 (3): 343–364.

Tschofenig, Hannes, Melanie Volkamer, Nicola Jentzsch, Simone Fischer Hübner, Stefan Schiffner, and Rodica Tirtea. 2013. *On the Security, Privacy and Usability of Online Seals: An Overview.* European Union Agency for Network and Information Security (ENISA). December. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/on-the-security-privacy-and-usability-of-online-seals/at_download/fullReport.

Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein. 2015. "Gütesiegel". Accessed November 1, 2015. https://www.datenschutzzentrum.de/ueber-uns.