EU Privacy seals project

Proposals and evaluation of policy options

Final Report Study Deliverable 4.4

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

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

2014

Report EUR 26834 EN

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

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

JRC Science Hub
https://ec.europa.eu/jrc

JRC91532

EUR 26834 EN

ISBN 978-92-79-40330-9

ISSN 1831-9424

doi:10.2788/14722

Luxembourg: Publications Office of the European Union, 2014

Abstract

This report examines some of the key EU level options and approaches that might be useful to consider and that fit the mandate set by the General Data Protection Reform on privacy seals, whilst at the same time are able to reconcile existing privacy certification initiatives and address the gaps and challenges identified in the existing privacy seals sector as shown in the reports of Task 1 (inventory and analysis) and Task 3 (gaps and possible scopes).

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

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

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

The authors of this report are:

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

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

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

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

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

Contents

List of tables

List of figures

1 INTRODUCTION

On 12 March 2014, the European Parliament voted in plenary with 621 votes in favour, 10 against and 22 abstentions for the General Data Protection Regulation and 371 votes in favour, 276 against and 30 abstentions for the Directive). The European Parliament backed the architecture and the fundamental principles of the Commission's data protection reform proposals, on both the General Data Protection Regulation (GDPR)[2] and on the Data Protection Directive in the law enforcement context. The GDPR, in particular, 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. Article 39 of the GDPR in particular, introduces the possibility of establishing certification mechanisms and data protection seals and marks.

Taking this into account, this report examines some of the key EU level options and approaches that might be useful to consider and that fit the mandate set by the GDPR on privacy seals, whilst at the same time are able to reconcile existing privacy certification initiatives and address the gaps and challenges identified in the existing privacy seals sector as shown in the reports of Task 1 (inventory and analysis) and Task 3 (gaps and possible scopes).

2 OBJECTIVES

The objectives of this report are:

- To determine how best to encourage the development of an EU-wide privacy seals scheme,
- To examine the key options that support the GDPR to this effect, identify their challenges, and assess their benefits,
- To provide some guidance and recommendations on how to implement these options.

3 METHODOLOGY

To attain the objectives of this task and analyse each of the options, we first developed a set of criteria (listed in section 4). These criteria focus on different elements relevant to privacy certification and are specifically suited to enable us learn more about the impacts of each of the options.

In Task 1 of the Study, we discovered that there are many privacy seals in existence.[3] One of the results of the task underlying this report (Task 4) is to show how the existing schemes might be included or involved in the EU-wide privacy seals scheme. In Task 2, we studied

[2] European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), A7-0402/2013, 21 Nov 2013.

[3] Rodrigues, Rowena, David Barnard-Wills, David Wright, Paul De Hert and Vagelis Papakonstantinou, *Inventory and Analysis of Privacy Certification Schemes: Final Report Study Deliverable 1.4,* Publications Office of the European Union, Luxembourg, 2013. http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26190/?CatalogCategoryID=CXoKABst5TsAAAEjepEY4e5L

established EU sectoral schemes and gained important insights on their working, success factors and challenges;[4] in this task, we transpose the lessons learnt from Task 2 into the options that are modelled on approaches similar to the schemes we analysed. The knowledge of how the sectoral schemes were created and the process of their implementation also informs this report.

Task 3 of the Study outlined the gaps of existing schemes and presented the possible scopes of an EU-wide privacy seals scheme. The results of that task (particularly in terms of contextual differences, potential barriers, targets of certification, policy, regulatory, technical and market requirements, roles and actions of stakeholders and sustainability)[5] also feed into this report.

4 CRITERIA FOR EVALUATING THE POLICY OPTIONS

This section sets out criteria for evaluating the policy options listed in section 5. We will examine each of the options in section 5 against the following:

1. Context, applicability (in line with legislative developments and technologies) and scope
2. Inherent risks and uncertainties
3. Obstacles to implementation
4. Role of different stakeholders (e.g. European Commission, national regulators, standards bodies, scheme operators, subscribers, relying parties, etc.)
5. Implementation, process, indicative implementation schedule, milestones, indicative timeframe for implementation
6. Impacts on:[6]
    a. *Individuals* (e.g., respect of data protection principles, protection and guarantee of data subject rights,[7] provision of means of disputes redress, support for consumer rights)
    b. *Relying parties or users* (e.g., trust and confidence in organisations, products and services)
    c. *Existing privacy certification schemes* (e.g., competition, additional burden to incorporate mandatory requirements, administrative burden, better privacy, data protection standards)

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

[5] De Hert, Paul, Vagelis Papakonstantinou, Rowena Rodrigues, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki, *Task 3 Challenges and Possible Scope of an EU Privacy Seal Scheme, D3.4, Final report*, Study on EU Privacy Seals, European Commission Joint Research Centre, Institute for Protection and Security of the Citizen, January 2014.

[6] The explanatory impacts listed under each of the sub-heads are only illustrative and not conclusive at this stage. These might vary according to the option. For instance sub-head (a) on data subject rights lists a number of rights of the data subject.

[7] For example: Right to know if an institution or body is processing data concerning him or her; right to information about the processing (about identity of data controller, purpose of processing, recipients of data, data subject rights), including automated processing and the relevant purposes; right to object to processing on compelling and legitimate grounds; right to prevent processing for direct marketing; right to object to decisions being taken by automated means; right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed and the right to claim compensation for damages.

d. *Certified entities or scheme subscribers* (large companies, SMEs, industry associations) (e.g., compliance, costs, resources, administrative burden, development of good practices, market benefits (image, turnover), competitive advantages, increase in process efficiency, enhance maturity levels of data protection management systems)
e. *Standardisation and certification bodies* (e.g., conflicting standards, support to existing initiatives, competition)
f. *Industry* (e.g., improvement in privacy and data protection, increase in awareness, discussion and good practices, increase in efficiency and image of a specific industry)
g. *Internal Market* (e.g., consolidation of the Internal Market, strengthening of the competitiveness of European companies, creation of conditions for economic growth)
h. *European society* (e.g., reduction of societal threat to privacy and personal data, increase in EU standards of privacy and data protection)
i. *Regulation and policy making* (e.g., relation to existing legislation[8] and interaction with existing mechanisms, policy-making impact, administrative impact and impact on compliance and enforcement)
j. *International community* (e.g., benefits for EU and Member States, export of high EU privacy and data protection standards, competition with existing schemes).

7. Evaluation and conclusion.

The criteria (developed based on Tender requirements) were revised and refined during the course of the research, and following discussions at the study workshop on *Considering Options for an EU Privacy Seal* hosted by the European Commission in Brussels on 8 April 2014.[9]

5 POLICY OPTIONS FOR CONCRETIZING PRIVACY AND DATA PROTECTION CERTIFICATION

This section outlines the specific options to be studied in this Task. Under the current GDPR mandate, a range of options is available for implementing an EU-wide privacy and data protection certification scheme. We analyse some of these options against the criteria listed in section 4. None of the options are mutually exclusive, and they might have some overlap – it may be possible to adopt one, some or a combination of options. Even within the options, different permutations are possible.

5.1.1 Encouraging and supporting the GDPR certification regime

[8] E.g. The European Parliament and the Council, 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, *OJ L* 218, 13 August 2008, pp. 30-47.
[9] The workshop aimed at sharing the results of the Study and gathering views on the options for EU privacy certification. Over 50 participants representing different stakeholders such as national data protection authorities, privacy seal issuers, industry, privacy associations, and academia, participated in the workshop.

This option envisages the Commission using various soft measures to stimulate and encourage compliance with the GDPR regime for certification and seals. This option explores what such measures could be (e.g. European Commission Communication, Recommendation, other soft law measures, further studies on certification mechanisms, seals and marks, and drawing up of codes of conduct). The aim is to encourage privacy and data protection certification through non-binding measures, including setting objectives and creating guidelines.

Context, applicability

Article 39 (1a) of the Parliament's version of the GDPR states:

> Any controller or processor may request any supervisory authority in the Union, for a reasonable fee taking into account the administrative costs, to certify that the processing of personal data is performed in compliance with this Regulation, in particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject's rights.

According to this, national supervisory authorities would be able to certify that the processing of personal data is performed in compliance with the Regulation. The Commission's role would be to encourage and support national supervisory authorities in this role, without additional institutional structures. If the Commission adopted a leadership role in this field, then the EU could set objectives and monitor progress towards these.

A second version of this option could see the Commission acting as a point of co-ordination for policy dialogue and information sharing relating to the national implementation of Article 39. The Commission could be involved in setting collective objectives for national supervisory authorities, commissioning and producing regular reports and studies 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. An advantage of this approach is that it could facilitate some measure of flexibility, and even experimentation, in methods of certification at the national level. Combined with appropriate co-ordination and sharing of best practices this might raise the overall quality of the regime over time. Activities in this direction could include networking, conferences, mutual review of national plans and strategies, roundtables, funding and commissioning of research projects, and national exchange projects.

The Commission has the capacity to issue Recommendations, including country-specific Recommendations. These are not legally binding, but do carry political weight. The intent is to offer advice to guide national policy.[10] The impacts of Recommendations are often subject to further monitoring to determine if additional (potentially regulatory) action is required. Recommendations might draw attention to problems or poor performance in national implementation efforts.

[10] European Commission, "Country-specific recommendations 2013: frequently asked questions" 29 May 2013. http://europa.eu/rapid/press-release_MEMO-13-458_en.htm

There are examples of soft law measures used by the Commission in the areas of state aid[11], social policy[12], research and innovation[13], telecommunications[14] and other areas. These examples suggest that the use of soft or hard law largely changes in response to the specific issues and context of a policy area[15], but that soft law such as rules of conduct with no binding force has played a practical role in European integration.

This approach could potentially involve an approach similar to the Open Method of Coordination (OMC). The OMC was established as part of the Lisbon Strategy to support the achievement of the Lisbon objectives of dealing with low productivity and stagnation of economic growth through iterative benchmarking of national progress towards European objectives and organised mutual learning.[16] The OMC consists of four elements:

- Fixing guidelines and specific timetables for achieving desired goals (including short, medium and long term).
- Establishing quantitative and qualitative indicators and benchmarks, tailored to the needs of Member States and sectors, in order to compare best practices.
- Translating European guidelines into national and regional policies by setting specific targets and adopting measures.
- Periodic monitoring, evaluation and peer review as a process for mutual learning.[17]

The OMC is an intergovernmental method, which would have to be significantly amended to take into account the role of data protection authorities and their relation to national governments. It could be envisaged that the European Data Protection Board (EDPB), with the involvement of member state expert, could perform all of the four functions listed above. There could also be a role for the Commission in terms of monitoring and setting the policy agenda. National supervisory authorities would be given (or retain) significant autonomy, in exchange for regularly reporting about their performance and activity, and participating in a peer review processes where these activities are compared with those of other national supervisory authorities. Jonathan Zeitlin, Professor of Public Policy and Governance, argues that based upon the available evidence, OMC has contributed towards, changes in national policy thinking changes in national policy agendas, changes to specific national policies, and procedural shifts in governance and policy-making arrangements in a number of sectors.[18]

Inherent risks and uncertainties

[11] Cini, Michael, "The soft law approach: Commission rule-making in the EU's state aid regime", *Journal of European Public Policy,* Vol. 8, No. 2, 2001, pp. 192-207.
[12] Trubek, David M., and Louise G. Trubek, "Hard and Soft Law in the Construction of Social Europe: The Role of the Open Method of Coordination", *European Law Journal,* Vol. 11, No. 3, May 2005, pp. 343-64; Jacobsson, K., "Beyond deliberation and discipline: soft governance in the EU employment policy" in Ulrika Morth (ed.), *Soft Law in Governance and Regulation: An Interdisciplinary Analysis,* Edward Elgar Publishing, 2004.
[13] European Commission, "Learning from each other to improve R & I policies". http://ec.europa.eu/research/era/partnership/coordination/method_of_coordination_en.htm
[14] Sabel, Charles F., and Jonathan Zeitlin, "Learning from Difference: The New Architecture of Experimentalist Governance in the EU", *European Law Journal*, Vol. 14, No. 14, May 2008, pp. 271-327.
[15] Cini, op. cit., 2001.
[16] Zeitlin, Jonathan, "Is the OMC an Alternative to the Community Method?" in Renaud Debousse (ed.), *The Community Method: Obstinate or Obsolete*? Palgrave MacMillan, Basingstoke, 2009.
[17] European Commission, "Learning from each other to improve R & I policies". http://ec.europa.eu/research/era/partnership/coordination/method_of_coordination_en.htm
[18] Zeitlin, op. cit., 2009.

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 taking into account that several countries have already developed structured privacy and data protection certification mechanisms, and that soft law mechanisms would have to integrate with these. Soft guidance from the Commission and/or the EDPB may be interpreted in different ways in different Member States, including the extent to which they are followed (although hard law is also not free from interpretative processes). This means that under this option particular attention should be paid to the coordination of the projects implemented at national level, and plans for convergence established. Even information and best practice sharing is unlikely to result in the transposition of an approach from one Member State to another. This would contribute another source of potential disharmony to the field of privacy seals (noting this is already characterised by high levels of heterogeneity), which may have negative impacts on citizens and consumers. Lack of specification is particularly problematic in policy sectors where there is a lack of information, and high complexity.[19] Coordination may be required as to who is eligible to subscribe to a scheme at national level, as data controllers and processors could request certification from any national supervisory authority in the EU, the distribution of awarded certifications in relation to the geographic and economic distribution of the certified entities may indicate which schemes attract most market support. However, forum shopping may be driven by increased benefits or lower requirements, in addition to reputation and recognition of various available schemes.

Recital 77 of the proposed GDPR indicates that a "'European Data Protection Seal' should be established on a European level". Under this option, such a seal could probably be a kind of umbrella certification mechanism, which national or European certification systems established by public or private bodies could adhere to. This would require some additional effort by institutional actors to bring about such an umbrella mechanism, and would be most similar to options three and four below.

In the absence of a fully-fledged and binding institutional system for checking and verifying compliance with the GDPR regime, this approach may lack weight. In order to guarantee transparency, specific mechanisms should be foreseen to ensure that one could verify that a certification has been awarded in line with recommendations made either by the Commission or the EDPB. The consistency mechanism built into the Regulation may help resolve this. Decisions with no EU-wide impact are taken at the level of individual DPAs, determined by the location of a company's main establishment, however, issues with an EU impact are subject to an opinion issued by the EDPB, with the Commission acting as a backdrop.

The reliance upon soft measures could leave open, to voluntary negotiations, a number of questions about the details of a certification scheme. Agreement should be reached on a case by case basis as regards many issues, for example, about what is to be certified, and what the criteria and requirements for certification would be. The Commission could produce guidance under this option; this guidance and support could be adopted or interpreted in different ways in different 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.

[19] Weber, Franziska, "European Integration assessed in the light of the 'Rules vs. Standards debate'", *European Journal of Law and Economics*, Vol. 35, 2013, pp. 187-210 [p. 190].

There is a risk that the soft measures may be ineffective. Similarly, this option may be interpreted as demonstrating an insufficient commitment to the certification process. Soft measures, including Recommendations, may be interpreted as avoiding politically sensitive consultations.

This option would require careful consideration about the best soft measure (or set of combined measures) to support and encourage the certification regime. This would probably depend upon the development of the certification regime and the activities of other stakeholders (in particular the activities of national supervisory authorities), such a policy option would more accompany the national developments in a bottom-up way, than impose a normative European approach, beyond what is required at national level. This option requires a decision to be made between the need for harmonised privacy certification schemes across Member States and the opportunity for policy innovation in this field. Given that some Member States have developed (CNIL, in France) or are developing (ICO, in the UK) their own privacy seal schemes, it suggests that there has been the potential space for policy innovation in the field by national regulators, but that this has not been attractive for the majority of national data protection authorities.

Obstacles to implementation

A key advantage of this scenario is flexibility and time to market as there are relatively few obstacles to the implementation of this option, and as the Commission and the relevant stakeholders could directly negotiate the implementation of a EU privacy seal, for instance as an umbrella supporting certification mechanism meeting a certain set of requirements. However, it may not meet several of the certification scheme success factors identified in previous tasks of this Study. In particular, this approach might not attain a sufficient harmonisation and a sufficiently clear and uniform framework of standards and criteria. It would lack additional legal rules which would increase the stability and potentially, effectiveness, of the regime. This being said, there are some examples of successful and harmonised data protection frameworks building on soft law guidance. The binding corporate rules (BCR) for international transfers are an example. Another example, in a related area, is the development of the RFID privacy impact assessment framework.

Similar approaches have been used in the past when the EU has lacked legislative competence in particular policy areas.[20] This is particularly true for issues such as privacy seals that would have a strong economic component.[21] OMC, and the use of soft law in general, has been criticised for being used in areas where the EU has legislative competence[22], and as being ineffective, although some authors have criticised this assumption on the basis of a lack of empirical evidence.[23] While the EU's legislative competence in the areas of privacy, data protection and standardisation is not in question, the issue is whether the EU could legislate in an area that is still embryonic, and whether an approach where the EU accompanies initiatives by DPAs and other bodies, might not be preferable, at least as a first step.

[20] Trubek and Trubek, op. cit., 2005.
[21] Van Hoboken, Joris, "The EU out of Focus: Some Deeper Truths about the European Approach to Privacy Law and Policy, *SSRN*, 31 March 2014. http://ssrn.com/abstract=2418636
[22] Zeitlin, op. cit., 2009.
[23] Ibid.

Article 39 (1) (c) of the GDPR suggests that a key mechanism for harmonisation would be co-operation between the national supervisory authorities and the EDPB. If the Commission was to adopt a soft measures approach, it would need to work in strong cooperation with the EDPB, national DPAs, and other stakeholders interested in the development of certification seals and marks to achieve the desired results.

This option potentially fails to address several gaps identified in the current landscape of privacy seals in the EU.[24] The certification provision in 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 five years under the Regulation, whilst the processes established by the national supervisory authorities would presumably exist in some form for the lifetime of the Regulation). Under such an approach, particular attention from the Commission in terms of a Communication and coordination could potentially help to address user trust and confidence in the schemes. However, even if the Commission is able to encourage harmonisation between national efforts, concerns are likely to remain in relation to the lack of incentives for the use and implementation of the scheme. The presence of multiple privacy seals schemes in the EU is unlikely to eliminate concerns of fragmentation, duplication of efforts and waste of resources. A 'soft law' endorsement by the Commission, the Member States and the EDPB of certain schemes meeting certain criteria might not achieve a sufficient level of harmonisation, and might even fail, if for instance some schemes that would not meet the requirements of the EU scheme are developed, undermining the European harmonisation effort.

As demonstrated in our previous reports, existing privacy seals schemes are fragmented, and duplicate effort. There are a multitude of seals, developed mostly locally in certain Member States often concentrated in a single sector (e.g. e-commerce). This option might not alleviate this, though it might ensure a high level of flexibility, and would require a constant dialogue between stakeholders.

Role of different stakeholders

We next outline the role of different stakeholders in relation to this option.

European Commission: Under this option the Commission would act as a coordination and leadership body, able to use its offices and other soft measures to support the development of coordinated certification schemes, or support the EDPB in this role. The main details of this role are set out in the first section of this option. Under this option, the Commission would not use its power 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, but would rather develop guidance together with other stakeholders, such as the EPDB. Such criteria might be specified by an Opinion, Recommendation or another Commission sponsored study, but would not have binding force.

EDPB: The burden of encouraging harmonisation of national processes could potentially be shifted to the EDPB rather than carried by the Commission. The EDPB would continue to

[24] De Hert, et al, *Task 3,* op cit., 2013.

carry the responsibility set out under Article 39 (1) (c) to cooperate under the consistency mechanisms to guarantee a harmonised data protection certification mechanism. The consistency mechanism (set out in Article 57 and Recital 105) envisages a mechanism for cooperation between the national supervisory authorities and the Commission, which can be invoked by supervisory authorities, the Commission and by data subjects if they deem that a measure by a supervisory authority or Member State has not fulfilled the criterion of consistency. The work carried out by the EPDB would be similar to that carried out in the context of the development of binding corporate rules. The EDPB and data protection authorities would rely on their general powers to ensure the proper development of data protection certification mechanisms in Europe and in their remit of competence.

National supervisory bodies/data protection authorities: If this option was adopted, national supervisory bodies would have to ensure that they are able to certify that the processing of personal data is performed in compliance with the Regulation or put sufficient measures and arrangements in place to be able to do this. Additionally, national supervisory bodies would participate in the collective setting of standards and benchmarks and the definition of objectives with the Commission. They would be expected to contribute examples of best practice and participate in the sharing of evidence and learning with their peers through this process.

Implementation, process, indicative implementation schedule, milestones

Implementation of this option would potentially be ongoing, and enacted as required to support the GDPR certification regime. If supporting activities are properly planned then they could flexibly respond to the ways that the certification regime develops over time. This would allow the Commission to take advantage of any "windows of opportunity" that arise in the sector.[25]

The timeline of such an implementation could be variable, however it is a rapid option compared to the other options in this study. The following milestones might be expected from the start of such an option. A potential first step in the first few months could be that the Commission would set up an expert group to support the development of guidance for seals providers. Early stages would possibly involve establishing a baseline understanding of how national supervisory authorities intend to meet the requirements of the Regulation. At this stage, it would also be possible for the Commission to exert influence on these strategies and plans as they were being formulated, perhaps through model suggestions and guidance. Later stages would involve monitoring how such strategies are progressing and establishing the best way for the Commission to support and encourage these efforts. This process would also need to include a review process to understand if this option was having the desired effect and to establish if a change in policy option was required. A further stage would be more evaluative, when one or more years of experience of operating under this regime had been collated and examined. This stage would allow reflection on the potential need for further or different policy measures.

This option is not inherently incompatible with other policy options, and could form part of a hybrid governance strategy, especially as it allows for much more aggressive implementation schedule as well as for much more flexibility than the other options/approaches.

[25] Cram, Laura, "The European Commission as a multi-organization: social policy and IT policy in the EU", *Journal of European Public Policy*, Vol.1, No. 2, 1994, pp. 195-217.

We estimate the timeframe for implementation of this option to be between 1-2 years.

Impacts on stakeholders

This section outlines the potential impacts of this option.

a. *Individuals:* Individuals might encounter a range of national certification processes and schemes which may be based upon divergent national implementations of the certification requirements. Whilst these may be harmonised and coordinated, there could be a strong centrifugal forces which could be difficult to address. This diversity may complicate the understanding of certification schemes and 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 and how it differs from other similar schemes.
b. *Relying parties or users:* Relying parties can be individuals (with the impacts addressed in the previous section) or organisations. Organisations may be able to identify, more effectively than individuals, the certifications most appropriate to them for their country and sector of operation. However, due to the limited harmonisation this option will bring about, there will be some information costs for organisations that rely on data protection certifications to find a scheme that offers adequate certification.
c. *Existing privacy certification schemes:* Existing privacy certification schemes, especially European schemes, could experience a growth in the number of their competitors as Member State supervisory authorities generate their own processes for the certification of data processing, as outlined in Article 39.
d. *Certified entities or scheme subscribers:* Data controllers and processors would be able to acquire certification from national supervisory authorities to certify that the processing of personal data is performed in compliance with the Regulation. This certification may grant them an advantage in the marketplace, increase trust from data subjects and allow them to demonstrate this certification to regulatory authorities. There may be less incentive to seek certification for compliance if it is only limited to a national interpretation of compliance, which may be divergent from the interpretations of the supervisory authorities in other Member States. Scheme subscribers may face the burden of seeking certification through different schemes in different Member States. As data controllers and processors could seek certification from any supervisory authority in the Union, they will also have to determine where it is appropriate to seek certification. It could be possible that certification requirements could be quite divergent in different jurisdictions (although they could 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.
e. *Standardisation and certification bodies:* National supervisory authorities may accredit specialised third party auditors to carry out the auditing of the controller or the processor on their behalf, although the final certification can only be provided by the supervisory authority. Existing certification bodies may be well placed to take on this role.

f. *Industry:* Many of the impacts upon certified entities and scheme subscribers listed above also apply to industry.
g. *Internal Market:* There is a potential for divergence and for less harmonised certification regimes to develop in Member States. Incompatible regimes may increase the burden on data controllers and processors operating in multiple Member States.
h. *European society:* This option will have some moderate impacts on European society in terms of potentially increasing EU standards of data protection through the basic provision of certification of data processing against the GDPR, which may in turn lead to better data and privacy protection, at least in relation to those data controllers and processors that seek certification. The soft measures and co-ordination 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 mitigate that. The diversity of implementation will possibly lead to an increased regulatory burden on European society as each Member State has to come to its own national arrangements to give effect to Article 39, and European society will have to manage the resulting complexity.
i. *Regulation and policy making:* This option is likely to have various moderate impacts on actors with responsibility for regulation and policy making, and will certainly require some effort on their parts. This effort will, however, be distributed amongst a number of actors at the EU and Member State levels, including national supervisory authorities. By encouraging the development of certification schemes, this option may contribute towards awareness of data protection, and the provision of mechanisms to verify commitments. However, it will not result in a reduced regulatory burden, and does include the potential for significant regulatory fragmentation if EU level co-ordination and information sharing measures are not sufficiently enacted.
j. *International community:* 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.

Evaluation and conclusion

Encouraging and supporting the GDPR certification regime is a relatively lightweight and flexible option, which is dependent upon the type of support activities that are put in place. The Commission can play a support role in this manner, 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 the expectations expressed for a European Data Protection Seal, the success factors previously identified in the Study, and fails to address existing gaps identified in relation to privacy seals.

5.1.2 Incorporation of EU data protection requirements into an existing EU certification scheme

This option involves introducing the requirements of the GDPR into one (or more) established certification scheme (such as those in the field of security or other relevant areas). This option envisages bridging Article 39 of the GDPR with other existing certification frameworks, leveraging them to boost privacy and data protection and, ultimately, adding value to them.

Our analysis here draws upon the analysis of existing privacy seals schemes (Task 1)[26] and their comparison with other EU certification schemes (Task 2).[27] We are therefore able to examine the suitability of a small number of existing EU certification schemes to "host" the EU data protection requirements as outlined in the GDPR.

As demonstrated by the analysis of existing privacy seal schemes in the first report of this study,[28] certification schemes do change over time, and this includes changes in their fundamental criteria.[29] This is necessary to reflect advances in technologies, or developments of new best practices within a sector. For-profit certification schemes may also change in response to customer demand or perceived demand from the market. Change over time is necessary to exploit the standards-improving policy role of certification schemes. The concept of regularly updated Best Available Techniques (BATs) is an example – here the standards underpinning certification schemes are regularly updated to drive, for example, the environmental and waste standards of industrial installation, as with the Integrated Pollution Prevent and Control (IPPC) certification.[30]

The appeal of this option comes from building upon the infrastructure and recognition of an existing, established scheme as a way of more rapidly and efficiently making EU data protection requirements certifiable. Incorporating EU data protection requirements into an existing EU certification scheme offers the opportunity of reducing the time-lag associated with the development and implementation of an entirely new scheme, and potentially reduces the risk that a new scheme would not attract adequate recognition and market acceptance. A new scheme might face the difficulty of becoming sustainable, whilst an existing scheme would have demonstrated that (at least in its current formulation) it is sustainable. Combining EU data protection into an existing certification scheme also offers certified entities the opportunity to meet several sets of standards or requirements at the same time, through a unified process. The administrative body of the existing scheme will also have accrued experience in certification which would prove useful in operating the data processing certification. There are also potential benefits for the certification body as there may be additional demand for the new certification.

Context, applicability

This option is not specifically outlined in the GDPR as such; however, it does not conflict with it in any manner. In taking into account its requirements, it would facilitate compliance with it.

The manner of the introduction of EU data protection requirements into an existing scheme would need some care and attention and this would be critical for the success of this option.

[26] Rodrigues et al, *Inventory and analysis,* op. cit. 2013.
[27] Rodrigues et al, *Task 2,* op, cit., 2013.
[28] Rodrigues et al, *Inventory and analysis,* op. cit. 2013.
[29] Ibid.
[30] Rodrigues et al, *Task 2,* op., cit., 2013.

Potentially, some additional authority would need to verify that the requirements had been incorporated properly into the existing scheme. Depending upon the existing scheme that is selected to "host" the new requirements, the scheme may call for an appropriate oversight body (perhaps at the EU level) or some temporary role for the Commission, Article 29 Working Party or the EDPB in helping the host organisation to incorporate the new data protection requirements, and verifying that this has been done appropriately, so as to sufficiently meet the new requirements. The EDPB may also play a role over time with regard to addition or removal of requirements from the scheme or other administrative changes.

Inherent risks and uncertainties

It would be necessary to determine which existing EU certification schemes could support the incorporation of EU data protection requirements. Options could include:

- An existing EU-located privacy certification scheme, operated by a third party (option 2.1)
- An existing EU-located non-privacy certification scheme, operated by a third party (option 2.2)
- An existing EU-administered non-privacy certification scheme (option 2.3)

These options would have different implications, but each would require potentially significant changes to the existing schemes. For both third-party administered schemes, the incorporation of EU data protection criteria would, in the absence of separate legislation, require some negotiation between the scheme administrator and relevant European stakeholders (e.g. the Commission, the EDPB, national data protection authorities) as to how the European requirements could be transformed into criteria or standards that could be certified against, and how these would be incorporated into the existing standards used by the certification schemes. This would introduce a high level of variability into the option, which would be strongly influenced by the extent to which the certification scheme was enthusiastic about the incorporation process. An unwilling third party, operating under pressure, could introduce substantial friction into the processes, or could result in the watering-down of the EU data protection requirements.

It would need to be determined if the EU data protection requirements were to be subsumed underneath existing certification criteria so that these requirements became part of any existing standard, or if the criteria were to remain separate, but the certification was to be administered and operated by the existing certification scheme, including its administrative and oversight bodies. The latter is distinct from the development of a standard through the ISO (or similar) process, in that it adopts an infrastructure for processing applications and granting certifications in addition to the development of a standard.

This option would create significant legacy issues that would have to be carefully addressed. Changing the requirements of an existing, established certification scheme causes some issues in relation to already-certified entities. Several schemes have simpler or more-relaxed requirements for re-certification in comparison to the initial certification process. Changing the requirements by adding additional, potentially complex, elements from the GDPR would potentially require that existing certified entities be re-certified to the new standard, which presumably (unless they were already prepared for the changes) some entities would be unable to meet. It may also create uncertainty for consumers and citizens in knowing which version of the scheme's criteria apply in a particular context. This impact may be reduced if

the selected scheme is one where knowledge of the detailed criteria is unimportant, but that mainly relies on the positive reputation of the scheme itself.

Related to sustainability is the issue of profitability of running the (expanded) certification scheme. For-profit certification schemes will have achieved some measure of calibration in relation to their market. The addition of new requirements and a resulting shift in the focus of the scheme may alter the estimations of potential certified entities, and may result in a change in the number of entities applying for certification. Both increases and decreases may have implications for sustainability and profitability (for example, a decrease in the number of applications may make the scheme unprofitable, whilst an excessive increase in applications may beyond the capacity of the scheme to adequately certify).

There is limited evidence on the impacts of significant changes in the role and focus of certification schemes, which places this option in somewhat uncharted territory. This option does not appear to have a significant number of comparable examples. The most detailed information on frequency and means of more minor updates to privacy seal schemes come from CNIL, EuroPriSe and the Japanese PrivacyMark scheme. 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 European 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)[31]. 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. With regard to non-privacy EU certification schemes, several schemes include mechanisms for regular updates to the criteria, and several have been changed by direct legislation, but we have not been able to identify examples of changes in requirements on the scale that might be required for this option.

Incorporation into an existing EU privacy scheme (Option 2.1)

Based on suggestions from the study workshop, we look at the expansion or development of the EuroPriSe seal as part of this option. EuroPriSe is a data protection and privacy-focused seal based in Germany that offers a European privacy and data protection certification scheme for IT products and IT-based services.[32] Evaluation of the certified product or service is conducted by external experts. EuroPriSe criteria are explicitly and directly based upon EU

[31] European Parliament and the Council, Directive 2002/58/EC 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 July 2002, p. 37–47.

[32] According to a press release, "the EuroPriSe seal and certification scheme will be transferred to EuroPriSe GmbH as of January 1, 2014. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD, Independent Centre for Privacy Protection Schleswig-Holstein) will transition management of the EuroPriSe seal and certification to EuroPriSe GmbH to further grow the premier European privacy and data protection certification for IT products and IT-based services". ULD, "EuroPriSe 2.0 – Continuation of the European Privacy Seal (EuroPriSe) by EuroPriSe GmbH – Extended range of certifications", 14 November 2013. https://www.european-privacy-seal.eu/ws/EPS-en/Press-releases

data protection law, in particular in Directives 95/46/EC,[33] 2002/58/EC and 2006/24/EC[34]. Having the support of a national data protection authority (the ULD serves as a Member on the EuroPriSe advisory board) and being aligned with data protection law make EuroPriSe a strong candidate for incorporation of GDPR requirements into an existing privacy seal. The revision and negotiation process would be much shorter than for many other schemes. Indeed in order to retain its key distinguishing feature of close alignment with European data protection and privacy law, EuroPriSe may attempt on its own account, to incorporate the novel elements of the GDPR that are not currently scheme requirements, into its criteria. However, whilst the scheme does have external experts located across Europe, only a very small number of entities have currently been certified under the scheme. If the EuroPriSe model was adopted by national supervisory authorities as the manner in which they would fulfil their obligation to provide certification then this might encourage more data controllers and processors to seek out EuroPriSe certification.

Incorporation into an existing EU non-privacy scheme (option 2.2)

Task 1 of the study examined the current alignment of existing privacy seals schemes with criteria derived from the GDPR. This was conducted as a fact-finding exercise to assess the readiness of these schemes to accommodate the GDPR criteria, rather than evidence of their success or failure in doing so. The general consumer-confidence and trust schemes did make some claims about privacy and data protection, however these were often minimal and under-detailed. The addition of GDPR-derived criteria to these schemes might serve to correct this lack *if* it was used as an opportunity to increase the attention these general schemes paid to privacy and data protection. However, such an addition would be a more significant shift away from the purpose and objective of the existing scheme than it would be for a scheme already focused upon privacy and data protection.

There may be sufficient overlap between privacy and security requirements that EU data protection criteria could be incorporated into an existing security certification scheme. As personal data cannot be adequately protected without security, and many documents and policies address security and data protection in combined form, it might be achievable to combine data protection requirements with an appropriately selected information security standard. For example, the Common Criteria have been developed for an objective evaluation of an IT product or system to assess whether it satisfies a defined set of security requirements. The Common Criteria certification is used for access control devices and systems, biometric systems and devices, boundary protection devices and systems, data protection, databases, detection devices and systems, smart cards and smart-card-related devices and systems, key management systems, multi-function devices, network and network-related devices and systems, operating system products for digital signatures and trusted computing. However, the Common Criteria does not have an EU foundation, with involvement from the US and Canada which may make it impossible to alter the standard to incorporate the GDPR requirements. ISO/IEC standards may be a better fit, and ISO 27000 standards series on the

[33] European Parliament and the Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *OJ L* 281, 23 Nov 1995, pp. 0031-0050.

[34] 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, 13 April 2006, pp. 54–63.

management and implementation of information security includes many controls and best practices which can contribute towards protecting personally identifiable information. However, information security and privacy are not commensurate and often have different organisational and individual foci. It is, for example, possible for personal data to be kept securely (preventing their access by hostile third parties, or their accidental publication) by an organisation that has collected them in a manner which violates individual privacy.

Incorporation into an existing EU-administered non-privacy scheme (option 2.3)

A third suggested option was the inclusion of EU data protection criteria into a certification scheme with high levels of consumer recognition. The argument here is that consumers will trust such a certification scheme, and incorporating data protection requirements into this certification will best serve the promotion of data protection, as well as providing the greatest benefit to certified entities (and thereby promoting uptake of voluntary certification). One such well-recognised scheme is the CE marking scheme. The CE scheme is a mandatory product labelling scheme under the responsibility of the European Commission. The presence of the scheme's logo on a product signifies the product's compliance with European legislation. It is intended as a multi-sector certification, although it currently only applies to manufactured physical products. Whilst devices can be designed with privacy and data protection in mind, the privacy and protection of personal data cannot be guaranteed on the basis of the electronic devices alone, but must also take into context the way that this device is used, in both individually, and in combination with a wide range of other devices and systems. Because of this, the dissonance between the current function, objectives, and target of the CE marking scheme, and what it would have to adopt to incorporate the GDPR criteria would be extremely large. In this context, the operational model of the CE scheme and the methods through which it has achieved consumer recognition may be better used as inspiration for the functioning of a European data protection seal scheme, rather than as a host for EU data protection requirements.

Obstacles to implementation

The initial obstacle presented by this option is that Recital 77 of the GDPR appears to call for the creation of "a European Data Protection Seal". However the "establishment" could be interpreted as any option that results in the establishment of an effective seal of this type, even if the origin is a pre-existing seal.

The current field of privacy seals, although diverse, may not be well placed to take on this requirement. The GDPR does not solely apply to data processing conducted in relation to websites, but many existing privacy seals are largely focused upon this. The existing European-based schemes are generally aligned with the current Data Protection Directive, although they have not generally automatically signalled compliance with the law. These schemes could potentially alter their certification criteria to include new elements of the GDPR. The EuroPriSe seal was intended to closely adhere to existing data protection requirements, but has a relatively small number of subscribers. This approach would also have to determine if the certification function could be fulfilled by a private-sector entity (the operators of most existing privacy seals schemes), although Article 39 (1) (d) of the GDPR does allow for independent third party auditors. Transparency is a requirement of Article 39 (1) (b) of the GDPR and existing seals schemes have been found lacking in this area.

This approach would require the willingness and the ability of the operators and legal authorities responsible for one or several existing EU certification schemes to incorporate EU data protection requirements into the scheme. The leverage of the Commission to encourage this may be highly limited, depending upon its relation to the administrative body of the existing scheme, but in the case of certification schemes already administered by the EU, this could be significant. The form of certification that appears to be envisaged in the GDPR is of compliance of data processing with the Regulation. This does not appear to allow for the certification of partial compliance, and by extension, if an accredited third party only certifies compliance against parts of the Regulation, then the national supervisory authority would retain the obligation to provide certification against other elements. This fragmentation of responsibility would be highly confusing for consumers, relying parties and for certified entities and should be strongly avoided.

Certification schemes may have their own internal processes for managing changes and updates to their standards (or they could in turn be reliant upon an external standard with its own change processes). This could delay the alteration of the scheme in comparison with the establishment of a new system.

Further, existing certification schemes have their own targets of certification, with their own inherent contexts. For example, the ISO 27000 family of standards is directed towards information security. Additionally, many certification systems are active policy responses to a specific set of issues in that context (the Green Dot scheme is intended to reduce packaging waste). Adding GDPR requirements to an existing certification scheme may distort the intended purpose of the existing scheme, or create a lack of clarity. It may also face resistance from organisations that are already using the standard for purposes related to its current focus, which find that they are now required to make changes to meet the new privacy requirements to retain the certification. The development of "pre-GDPR" and "post-GDPR" versions of the standard in circulation and use should be minimised. A standard which is commonly re-assessed on a yearly basis would be preferable to a standard where a longer lifespan is more conventional, to minimise this risk.

Article 39 of the GDPR specifies that certification should remain valid as long as the processing operations are in compliance with the regulation, up to a maximum of five years; that the supervisory authorities themselves must formally issue the seal or certification, and that there be a publicly accessible register of valid and invalid certificates. An existing scheme may have to be reformulated or expanded to take these legal requirements into account. Similarly, the scheme would have to be available to data controllers in all EU Member States and be sufficiently established at the European level.

Role of different stakeholders

EDPB: As a body with expertise on privacy and data protection, as well as a membership composed of European data protection authorities, the EDPB would be a suitable point of co-ordination for the assessment of suitable schemes, as well as verifying that the expanded certification criteria satisfy the requirements of EU data protection law.

European Commission: The Commission could exercise an oversight and co-ordination role in the identification and selection of an existing EU certification scheme to which data protection requirements would be incorporated. If the Commission is responsible for the operation or governance of the appropriate scheme then they will take the lead role in the

revision of the certification scheme's criteria and, of any operational aspects that will needed to be adopted to satisfy the requirements of Article 39 of the GDPR.

National supervisory authorities: Given the role of national supervisory authorities in investigating compliance with data protection law, it would be advantageous for national supervisory authorities to retain some ability to revoke certifications from data controllers and processors otherwise found to be in violation of the European data protection law.

Implementation, process, indicative implementation schedule, milestones

It would first be necessary to assess the potential candidate certification schemes for their compatibility with the GDPR requirements. This would also include the identification of capable schemes where it would be functionally feasible to incorporate the scheme and where the EU might be able to encourage or ensure that this occurred. If the ideal scheme was outside the direct control of the EU, then a period of negotiation between the scheme and the relevant bodies would have to occur. This process may have to proceed in parallel with more than one potential candidate scheme. Once a candidate scheme or schemes have been selected, the revised certification criteria would have to be developed and then approved, probably including consultation with stakeholders. Once the criteria is developed and accepted, it would then have to be publicised and made available to potential certified entities. Depending upon the origin and scope of the selected schemes, there would potentially have to be some recertification of existing certified entities of the host scheme, as well as potentially efforts to expand the certification scheme to other Member States. Unless all existing certifications under the scheme are revoked or invalidated at the point of incorporation of the new requirements, there would also be an overlap period, during which the certifications of existing certified entities are still valid, and new certifications are being issued. Depending upon the validity period of the certification, this would possibly be just less than one full year from the point of publication of the new criteria. Depending upon the time taken to produce the new criteria, and how public this process was, there may be a decrease in the number of newly certified entities in this run-up period, as entities wait for the release of the updated criteria. Currently certified entities might possibly maintain their certification up to this point.

Parallel to this process, other existing privacy certification scheme providers may start to include GDPR requirements into their certification schemes on their own initiative after the Regulation comes into effect. They may anticipate that being able to certify compliance with the requirements of the Regulation may be of benefit to their customers and therefore seek to provide this. This is particularly relevant for schemes where privacy is a core focus (as opposed to broader trust and security schemes with a privacy dimension) and those schemes where alignment with EU privacy and data protection legislation is a key selling point. There is an obvious overlap here with schemes that would have been candidates for the inclusion of GDPR criteria. This additional and multiple incorporation may create some confusion in the marketplace if there is also an officially sanctioned and supported incorporation of the requirements into a specific scheme.

We estimate the timeframe for implementation of this option to be between 2-3 years.

Impacts on stakeholders

This section presents the impacts on relevant stakeholders:

a. *Individuals:* To the extent to which this option fulfils the objectives of Article 39 of the GDPR, individuals would have access to a system whereby data controllers and processors offering services to those individuals could demonstrate their compliance with EU data protection law. This could create increased trust and confidence in those data controllers and processors and increase the uptake of useful and beneficial services by individuals. This option does, however, create the potential for confusion between the previous version of the certification scheme and the expanded version including data protection criteria. Many non-expert users, who are not acting as relying parties may be unaware of the change in certification criteria, but are unlikely to be actively harmed by this.
b. *Relying parties or users:* There is a potential for significant uncertainty on the part of relying parties. Relying parties can be separated into two groups. The first group is those who were reliant upon the scheme for some purpose before the incorporation of existing standards. These purposes may still remain valid, if existing criteria have not been removed from the standard. For example, if a relying party was using an information security standard to ensure that companies it dealt with had information security policies in place, then this would still be the case. The second category of relying parties is those who have a particular interest in the new privacy and data protection criteria. Whilst these parties would have access to and benefit from a certification scheme with increased relevance to their interests, they would be potentially vulnerable to confusion and misdirection during the overlap period.
c. *Existing privacy certification schemes:* This option would have a large impact here, particularly upon the scheme(s) that were selected to incorporate the GDPR criteria. There would potentially be impacts upon the branding and marketing of the certification scheme, as well as upon its administration, profitability (if it is a for-profit scheme) and sustainability. To meet some of the requirements for legitimacy set out in the rest of this section, the scheme would acquire additional oversight from the EDPB (and/or potentially from the Commission) as well as a new set of partnerships with national data protection supervisory authorities. This option could also have a negative impact upon schemes that were not selected as they would potentially be seen as less valuable than a scheme that signalled full compliance with the new legal requirements.
d. *Certified entities or scheme subscribers:* May require re-certification under the expanded or adjusted scheme criteria. Some certified entities will be able to alter their practices so as to conform to the new criteria and maintain their certification were as others may have more difficulty and may find their certification revoked. Depending upon the administrative changes brought about by the incorporation of the new requirements and for certification against them, administrative processes related to the scheme (including fees and charges) may change. Certified entities will have to assess and decide if the new version of the scheme is still an appropriate fit with their goals and objectives and if certification is worth pursuing.
e. *Standardisation and certification bodies:* Depending upon the scheme selected to host the incorporated data protection standards, relevant standardisation bodies may be required to adjust their standards to include these requirements. Certification bodies may be required to become skilled in conducting the

functional assessment and evaluation of data processing compliance against these standards. These types of bodies have experience in these fields.

f. *Industry:* Industry would gain access to a route to certification of compliance with EU data protection principles which could prove valuable in demonstrating good faith towards potential customers, and demonstrating their capacity to investors and clients. The scheme would remain voluntary, and it would be up to individual firms to determine if certification was appropriate for them, although they would be legally obliged to conform to EU data protection law if operating within the EU.
g. *Internal Market:* There is a danger in this option that the national supervisory authorities of some Member States might adopt the expanded certification scheme as their mechanism for meeting any potential obligations for the provision of certification, whilst other Member States adopt a different mechanism. This may have implications for harmonisation and subsidiarity, although given that the GDPR is a Regulation, it would apply in all Member States, and certified entities may be able to apply to the scheme directly, regardless of the Member States in which they operate.
h. *European society:* Could broadly benefit from many of the potential goals of privacy certification in the general improvement of privacy and data protection standards, and the confidence in information technology-related business that can be associated with this.
i. *Regulators and policy makers:* Are able to reduce some of the risks of starting an entirely new privacy certification scheme and pass on some of the responsibility for administration of the scheme to the existing organisation and administration (which may be other regulators and policy makers, depending upon the selected scheme).

Evaluation and conclusion

The incorporation of EU data protection requirements into an existing EU certification scheme is a potentially complicated policy option with a large number of uncertainties and potentially disruptive impacts on stakeholders. While it offers a way of leveraging existing certification or seal scheme recognition in support of data protection certification, it is not clear that this would be a significant enough benefit, given its potential to cause confusion for individuals and relying parties, and the possible negative effects on an existing successful certification scheme. Schemes that are established seem an inappropriate fit for the EU data protection principles, whilst existing schemes that would be a good fit currently have a low uptake. These latter schemes could however benefit from the extended institutional support and attention that such a formalised incorporation, with support from key EU actors and national supervisory authorities, could bring.

5.1.3 Accreditation of certifiers by an EU-level body: 'certify the certifier'

Accreditation means attestation by an accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity. Based on the scope of the study, this option analyses the accreditation of privacy certification schemes by an EU-level body.

As shown in Task 1 of the Study, there are a number of privacy seal schemes operating within the EU. However, none of these are harmonised in their criteria, process or targets of evaluation. There is no means for individuals or other relying parties to assess the credibility of the privacy certifier; specifically, whether the privacy certifier adequately assesses and ensures its certified entities guarantee (or even can guarantee) the protection of privacy and personal data in line with EU law. There is also the problem of trust – which comes from being able to know whether the certifier has somehow favoured the certified entity, is competent enough to perform its task, and exercises the required level of care in performing its tasks. Lack of trust is significantly detrimental not only to individuals in particular, but society in general. Therefore, some means of accreditation (an assessment of the technical competence and integrity of the organisations offering privacy and data protection certification and seals) is important. This would benefit the privacy certification sector, with the underlying goal being to improve the quality of privacy certification and/or seal offerings.

This option envisages a specialist EU-level body or organisation (either new or existing[35]) accrediting privacy seal schemes against the criteria set either by the Commission or the European Data Protection Board (EDPB), (or against another agreed EU standard) for privacy seals.[36] The argument supporting the involvement of these organisations is that they possess specialist expertise in data protection. Existing privacy certification schemes could voluntarily apply to be accredited, and if found compliant with the set criteria and requirements, would be certified or awarded the EU privacy seal. Non-EU based schemes could also apply for accreditation. The objective of this option is to promote harmonisation in EU privacy certification schemes, facilitate consistency in their offerings and practices, improve the quality of existing certification schemes, and foster trust and confidence in them. Under this option, existing schemes could become a part of an EU umbrella framework or system for privacy certification.

The criteria for accreditation of privacy seal schemes could be established by the Commission. The Commission would also establish the basic aspects of the accreditation process and system. Alternately, the criteria and requirements could be set by the EDPB. Either way, the criteria and requirements should at least take into account:

- the general principles of EU data protection (as finally embodied in the GDPR) and privacy law,
- independence (financial[37] etc.) and impartiality of the certified scheme[38],

[35] It might be possible to extend the mandate (to cover accreditation of privacy certification schemes) of the European co-operation for Accreditation (EA) which currently coordinates and leads the European accreditation infrastructure. The EA accredits the following certification bodies: product Certification (EN45011- ISO/IEC 17065), certification of persons (ISO/IEC 17024) and the Management Systems Certification (ISO/IEC 17021). The EA is an association of national accreditation bodies in Europe that are officially recognised by their national Governments to assess and verify, against international standards, organisations that carry out evaluation services such as certification, verification, inspection, testing and calibration (also known as conformity assessment services). http://www.european-accreditation.org/about-us

[36] It is important that the criteria setting body and the accreditation body are different to ensure that there is no bending of rules or compromise of the underlying objectives of the accreditation.

[37] This means that the certifier is financially independent, its funding is not dependant on the commercial interests it assesses, that it has no brokerage or ownership interests in the products or services it certifies.

[38] Threats to impartiality might include: self-interest threats, self-review threats, familiarity (or trust) threats, and intimidation threats. (ISO/IEC 17021 - Conformity assessment — Requirements for bodies providing audit and certification of management systems).

- competence (demonstrated capacity to consistently achieve stated policy and objectives, repeatable assessment processes and procedures),
- quality of services,
- establishment and maintenance of a system capable of supporting and demonstrating the consistent achievement of accreditation criteria,
- transparency,[39]
- existence of disputes redress process and mechanisms,
- responsiveness to complaints[40],
- surveillance mechanisms, and
- policy and documented procedures for suspending, withdrawing or reducing the scope of certification.[41]

Whatever the criteria (and we suggest that this option should take into account relevant international standards such as ISO/IEC 17021:2011 Conformity Assessment - Requirements for bodies providing audits and certification of management systems[42]), they have to be optimal to the objectives of the scheme and be achievable. The accreditation process itself would have to be well-established, rigorous and transparent.

The EU-level body responsible for the accreditation will actively monitor and oversee the administration of the overarching scheme and conduct the market surveillance to ensure that the scheme is not misused in any manner. It (or the Commission) should maintain a register of all the accredited EU privacy certification schemes (and possibly inform the public of any malpractices). The Register would be the 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 about whether a particular privacy certification scheme met the high EU standards or not.

The scheme might envisage the issue of an EU seal signifying the accreditation. For example, an existing privacy and data protection seals provider might be accredited and awarded the seal which it could display on its website or use it for marketing purposes. Schemes could be accredited for either a period of three to five years. The European scheme operator would be entitled to conduct random audits of the individual participating schemes. However, these schemes should be obliged to inform the accrediting organisation of any changes to their policy, practices and procedures that impacts their accreditation in any way.

[39] E.g. ISO 17021 states that a certification body needs to provide: public access to, or disclosure of, appropriate and timely information about its audit process and certification process, and about the certification status (i.e. the granting, extending, maintaining, renewing, suspending, reducing the scope of, or withdrawing of certification) of any organisation, in order to gain confidence in the integrity and credibility of certification.

[40] ISO 17021 states that "parties that rely on certification expect to have complaints investigated and, if these are found to be valid, should have confidence that the complaints will be appropriately addressed and that a reasonable effort will be made to resolve the complaints. Effective responsiveness to complaints is an important means of protection for the certification body, its clients and other users of certification against errors, omissions or unreasonable behaviour. Confidence in certification activities is safeguarded when complaints are processed appropriately."

[41] This is an indicative list at this stage.

[42] ISO, *ISO/IEC 17021:2011 Conformity assessment -- Requirements for bodies providing audit and certification of management systems,* Stage: 90.93, 17 January 2013.
http://www.iso.org/iso/catalogue_detail?csnumber=56676

This option considers both the priorities not only identified in the proposed GDPR, but also the priorities identified in the Study (Task 3).[43] The above specified nature of the scheme will provide several advantages. It would provide a means of demonstrating which privacy certification schemes (and their underlying criteria and practices) are acceptable and trustworthy in the EU. It would help accredited privacy certification schemes differentiate their offerings from other schemes. It also provides an alternative means of ensuring the reliability of privacy certification schemes which have implications for public trust and confidence. This option could provide a visible, easy and reliable means of identifying schemes that meet and maintain high EU standards. The public will be able to know that accredited schemes and their logos are trustworthy and can make more informed choices about which seals to trust and which they should not.

Context, applicability and scope

This option permits existing schemes the option of joining an EU umbrella. 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). This option helps eliminate this problem. This option will provide existing privacy seal schemes with a framework against which to evaluate their offerings and bring their practices in line with EU requirements and standards, and societal expectations, which can then percolate down through the privacy seals chain to the end relying party.
This option would address the gaps we identified in Task 3 of the Study in a number of ways. First, its pre-set criteria and administration by an EU-level body would facilitate a harmonised approach and protection of personal data across the EU. The Register of certified schemes would help boost user trust and confidence and reduce the deceptive effects of schemes. The EU-wide scope of the scheme and its potentially exclusive nature (there is no EU-level scheme providing accreditation of privacy certification schemes) is an incentive for its use. Further, as it will be established at the EU level, it is less likely to have a transitory nature (as has been seen in relation to nationally scoped schemes). It also has a global scope.

Inherent risks and uncertainties

This option might require the setting up of a new EU-level organisation to administer the scheme. There are many possible legal forms for such an EU-level organisation; ranging from a non-profit organisation, private company or an EU agency established in a dedicated legal base. This would entail a significant resource burden, particularly in terms of the costs and take some time. The choice of the legal form of the organisation responsible for the accreditation will also require a careful further assessment. These may prove to be prohibitive and it may not be acceptable that those costs should be covered by the EU budget. The EU-level body or organisation responsible for the scheme would require adequate resources, and certification and data protection and privacy expertise. It would also need to be sufficiently impartial and independent, and to be seen as such.

The criteria for accrediting privacy seals would need to be developed to a high EU standard, and in line with EU societal expectations, albeit with the potential to allow schemes to innovate and grow.

[43] De Hert, et al, *Task 3*, op. cit., 2013.

Obstacles to implementation

The scheme is intended to be primarily voluntary. Unless there are legal, economic or competitive advantages, privacy certification schemes might not see value in applying for accreditation. Additionally, the interplay between the accreditation system and the 'free market' competition between certification schemes may prove difficult to manage. Further, it is not clear whether existing privacy seal schemes would be willing to open themselves, their criteria, processes and procedures to scrutiny. This might then result in the need to support the scheme by mandating accreditation of all privacy, data protection schemes operating in the EU.

Role of different stakeholders

We envisage the following roles for the different stakeholders in this option:

- **Scheme operator (accrediting body)**: to efficiently perform its task of accrediting privacy certification schemes to the set criteria and requirements. The scheme operator must be independent from the privacy seals schemes it accredits. It must be objective and impartial. It must employ competent personnel to carry out its tasks. It should operate on a not for profit basis. It must not offer services offered by privacy seal issuers and it must not compete with other accreditation bodies.
- **European Commission:** The EC may need to set out the criteria and conditions (and process) for accreditation in a dedicated act. It would review and update the criteria and conditions, as required to optimise the objectives of the scheme and in line with legal and societal goals. In addition the Commission may need to support standards organisations with the development of the criteria and requirements for the scheme. The EC may also have to regulate on the revocation of an accreditation, and/or the removal of a certification mark.
- **EDPB:** could be responsible for determining the criteria and requirements for the accreditation.
- **European Standards Organisation:** The European Standards Organisations could help develop the criteria and requirements for the scheme.
- **Privacy certification schemes**: would apply for accreditation. The successful acquisition of accreditation will provide them with a competitive, reputational advantage over non-accredited schemes and increase their relevance throughout the internal market. The schemes will be responsible for ensuring that their policies and practices are in line with the accreditation
- **Relying parties, individuals**: would check whether privacy certification schemes are on the register of accredited schemes.
- **National supervisory body**: No additional burdens (of course under their general remit, DPAs could be vigilant against schemes that violate their accreditation obligations). DPAs could also encourage schemes to become accredited as a measure of good practice.

Implementation, process, indicative implementation schedule, milestones

We envisage the following steps in the implementation of this option:

- Setting up of the EU-level accreditation body

- The development of the accreditation criteria
- Pilot of the accreditation with some existing privacy certification schemes
- Post-pilot review and amendments to scheme
- First wave of accreditations
- Launch of the Register

The accreditation process under the scheme would involve the following steps:

1. Application for accreditation (in the prescribed form, and according to a set process supported by relevant documentation)
2. Pre-assessment (the main purpose of the pre-assessment might be to clarify needs and make a preliminary identification of any issues that can be addressed before a full assessment).
3. Full assessment
4. Accreditation decision
5. Publication on the register
6. Maintenance of accreditation

Each of these steps will have resource implications. We estimate the timeframe for implementation of this option to be between 3- 4 years.

Impacts on stakeholders

We now outline the impacts of this option on relevant stakeholders:

a. *Individuals:* This option will present individuals with the means of assessing privacy seals with greater confidence; something that is still not sufficiently within their reach. It will help individuals decide and discern about which privacy seal schemes to trust or not.
b. *Relying parties or users:* It might lead relying parties and users of privacy seals to demand that privacy seals get accredited under this option. In the same way as individuals, relying parties will have more or better assurance about the claims being made, especially in cross-border contexts.
c. *Existing privacy certification schemes:* If this option is made mandatory, there will be accreditation resource burdens for all privacy certification schemes; if non-mandatory, there will be resource burdens for those that apply for accreditation. This might mean that only schemes that can devote time, other resources and are open to the idea of being accredited will apply. Accredited schemes might gain a competitive and reputational advantage over non-accredited schemes – in turn, they may be able to use their accredited status to draw in greater number of applicants, not only from their country of establishment but also 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. One other important impact is that if it turns out that due to costs involved, non-accredited schemes are cheaper to subscribe to that accredited ones, accredited schemes might lose business and this might impact the potential of this option.

d. *Certified entities or scheme subscribers:* will be able to trust and have greater confidence that the scheme they are applying to have been accredited and meets EU standards and requirements. Thus, they may show greater willingness to apply and continue to remain a part of schemes that have been accredited in line with this option.
e. *Standardisation and certification bodies:* As of writing, there is no EU standard for accrediting privacy certification schemes. One alternative is to get the European standards bodies to contribute to the development of the criteria for the accreditation of privacy seal schemes.
f. *Industry:* This option will help address the gaps identified in the privacy seals sector and help schemes to grow. In enabling schemes to open up their criteria and practices and in harmonising the EU-level criteria, it will facilitate and improve privacy and data protection, efficiency and boost the image of privacy seals.
g. *Internal Market:* This option is in tune with the goals of the Internal Market. It will strengthen the competitiveness of European privacy certification schemes, and create desirable conditions for their economic growth, though questions of subsidiarity may arise in relation to whether an EU-privacy seal scheme could be achieved without a centralistic approach.
h. *European society:* The current privacy seals scenario is an unregulated free-for-all, with schemes free to define their criteria and operational practices; this option will present EU society with the means (through a dedicated EU-level body and pre-defined criteria and requirements) to benefit from possibly a more harmonised, regulated and trustworthy privacy seals sector.
i. *Regulation and policy:* This option will require new policy and regulatory measures. There will be an administrative impact in terms of costs.
j. *International community:* This option will show the leadership of the EU in harmonising its privacy seals sector. This option might also present benefits to international consumers who rely only on seals that are registered on the EU Register.

Evaluation and conclusion

This option is a novel one; there is currently no scheme that accredits privacy and data protection certification schemes at the EU level to pre-defined EU criteria and requirements.

While certification might be viewed often as a purely commercial activity, this option, which involves accreditation of privacy certification schemes by an EU-level body, is not of that nature. This option should be carefully exercised. Its ultimate success will depend on whether it brings added value, is sustainable in the long run and helps generate more confidence and trust in privacy and data protection certification (mechanisms, tools and players).

5.1.4 Creation of a harmonised standard for EU privacy seals

This option envisages the creation of a harmonised European standard or family of standards for privacy certification schemes through the European standardisation (EN) framework. This standard would be applicable to privacy, data protection certification schemes offering their services within the EU. For this option, standardisation is seen as a tool to integrate existing privacy certification schemes and provide a harmonised reference point against which these

schemes can be evaluated and assessed. Currently, no such specific standard exists. [We acknowledge the existence of ISO/IEC 17021:2011 which contains the principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types (e.g. quality management systems or environmental management systems) and for bodies providing these activities[44]].

As clarified by the European Commission's *Vademecum on European Standardisation*, the Commission could ask the European Standards Organisations or ESOs (CEN, CENELEC, and ETSI) through a mandate[45] to draw up technical specifications, for a harmonised standard for privacy, and data protection certifiers in the EU, that meet the Commission's requirements.[46] It would be the Commission's responsibility to lay down strict requirements to safeguard the public interest (specifically, ensuring that privacy certification schemes have adequate processes and criteria in place that enables their subscribers to comply with EU data protection and privacy law). The ESOs are responsible for drawing up suitable standards that meet these requirements and take account of the "state of the art".[47]

The concept of a mandate is based on the principle of partnership, cooperation and the clear division of tasks between the public authorities and the duly recognised European standardisation bodies.[48] There are three types of mandates: study mandates, programming mandates and standardisation mandates. The study mandate aims to determine if European standardisation is relevant and feasible in a specific field or for a certain subject. This type of mandate is most common in non-regulatory fields or for new sectors. The programming mandate asks the European standardisation bodies to draw up a standardisation programme in a given time. The programme has to contain *inter alia* the subjects to be standardised, the relevant technical organisations as well as the completion dates laid down. It can also include an inventory of the existing standards to be revised to meet the set requirements. A standardisation mandate calls on those drawing up standards or other alternative standardisation deliverables to prepare and adopt within a given time European standards in a specific field, possibly on specific subjects. Apart from these three types of mandates, there are also "combined" mandates which involve asking the European standardisation bodies to prepare in a first phase a work programme and in a second phase the implementation of this programme. The Vademecum clarifies that "each mandate should not solely describe which requirements and which criteria of the standards or alternative standardisation deliverables need to be satisfied, but must also include the elements allowing and facilitating the monitoring of its implementation".[49] This facilitates the detection of possible gaps in the standardisation work compared with the mandate and the related New Approach Directive.

---

[44] ISO, *ISO/IEC 17021:2011 Conformity assessment -- Requirements for bodies providing audit and certification of management systems*, Stage: 90.93, 17 January 2013.
http://www.iso.org/iso/catalogue_detail?csnumber=56676

[45] European Commission, Enterprise and Industry, Directorate-general, New Approach Industries, Tourism and CSR Standardisation, *Vademecum on European Standardisation*, Part II, European standardisation in support of European policies, Chapter 4.1, Role and preparation of mandates, 15 October 2009.
http://ec.europa.eu/enterprise/policies/european-standards/files/standards_policy/vademecum/doc/preparation_of_mandates_web_en.pdf. The Vademecum states, "Mandates must be regarded as the framework which refers to the public interest requirements and which enables the standards bodies to develop quality standards that meet these requirements".

[46] These refer to the Commission requirements representing European law and social assumptions as in the previous option.

[47] EC, *Vademecum*, op. cit., 2009.

[48] EC, *Vademecum*, op. cit., 2009.

[49] Ibid.

The Commission's request would include detailed guidelines which the requested standards must respect to meet the essential requirements or other provisions of relevant European Union harmonisation legislation, in this case, those embodied in the General Data Protection Regulation.[50] A European Standard (EN) automatically becomes a national standard and therefore is included in the standards catalogue of CEN's Members, the national Standardisation organisations in 33 countries. European Standards are drafted in a global perspective and CEN is signatory to the 'Vienna Agreement' with the International Organization for Standardization (ISO) through which common European and international standards can be developed in parallel providing dual benefits of automatic and identical implementation in CEN Member countries, and global applicability.

This option is different from the previous option (accreditation of certifiers) in that it does not involve the creation of an EU-level body, only chooses to harness the existing EU standardisation organisations to develop a harmonised European standard for privacy certification schemes. The standard developed in this option could be used as a basis for accrediting privacy certification schemes in the previous option.

Context, applicability and scope

The harmonised European standard for privacy certification schemes would represent a model specification which privacy or data protection certification schemes in the EU should meet or against which they could be assessed. It would codify best practice and state of the art in privacy and data protection certification, with a focus on the priorities underlined in the General Data Protection Regulation (and those specifically highlighted in the Second Interim Technical Report of this Study, as outlined later in this section).

There are two alternatives in using the Standard, post-development. One alternative is that it is left to national accreditation bodies to evaluate and assess privacy and data protection certifiers that apply to them for such certification. The other alternative (as envisaged in option 3), is for the Standard to be used by the specialist EU-level body or organisation to accredit privacy certification schemes in the EU.

While the core target of this option is to address the lack of harmonisation and common standards in privacy certification in the EU, this option is also suited to address the following gaps that the Study identified relation to existing privacy certification schemes: Lack of transparency (including the criteria used to award seals, target of certification), abstract claims, lack of appropriate level of data protection, deceptive potential of schemes, close relationships between schemes and members, schemes justifying increased collection and processing of personal data, and enforcement issues.

This option has the potential to enhance accountability, transparency of privacy certification schemes and reduce fragmentation and duplication of efforts. However, along with the priorities outlined in the General Data Protection Regulation, it should take into account the following priorities identified in the Study: appropriate level of privacy and data protection for individuals, enhancing the internal market dimension, standardised approach for the EU, specificity and guidance, transparency, accountability, and public awareness and trust.

[50] Prior to the issuing a standardisation mandate, the Commission could issue a study mandate asking the ESO's to check the feasibility of European standardisation for privacy certification schemes.

Inherent risks and uncertainties

European standards, even if developed under a mandate and supported by EU legislation, are expected to remain voluntary in their use. Their value could be enhanced by reference to them in legislative texts (viewed as a more effective means of ensuring compliance with legislation than the writing of detailed laws). This would help both processes to "support each other, without causing a slowdown".[51] It is also 'softer' and more co-regulatory than a full regulatory approach.

Standards setters are often attributed with "working in an area of imperfect knowledge, high economic incentives, changing relationships, and often, short-range planning".[52] The harmonised standard for privacy certification schemes might not be per se 'public facing'; it may be more technical and less known to the public and media. However, since the standard aims to be an open standard, it will help eliminate any concerns about its transparency.

Negotiating standards is a difficult task. There is the problem where "the more parties involved in negotiating standards the weaker the standard tends to become and the longer it takes to finalise".[53] This option will have to act to eliminate the bias in favour of the technical competence and political importance of some of the major, influential stakeholders involved in this process.

A European standard might have the propensity (due to its need for flexibility) to be weak. If the standard is kept vague or abstract, it risks becoming open to variant interpretations. This will be harmful for the end objective of enhancing data protection and privacy.

Obstacles to implementation

This option does fit in with the spirit of the proposed General Data Protection Regulation. However, its inherent risks and challenges do pose some concerns that would need to be addressed. If these are not addressed, they will impede successful implementation.

In theory, the ESOs could refuse a mandate if they do not think that standards can be produced in the area being covered (this is rare) or may ask for changes to the mandates with the view of their acceptance.

There might also be opposition from industry (particularly the privacy certification sector), if the Standard does not provide added value to them or they feel threatened in some manner (i.e. the Standard imposes unreasonable demands or somehow restricts growth and innovation). Past experience has shown that industry stakeholders might get too involved in the process and try to steer it in their preferred direction. Whilst the standardisation process would need their input (and their eventual buy-in) it is important to ensure that the core aims of encouraging data protection and privacy of individuals through the support and

[51] CEN, "CEN Compass: The world of European Standards". http://www.din.de/sixcms_upload/media/2896/CEN_compass.pdf

[52] Cargill, Carl F., "Why Standardisation Efforts Fail", *Journal of Electronic Publishing*, Vol. 14, Issue 1, Summer 2011. http://quod.lib.umich.edu/j/jep/3336451.0014.103?rgn=main;view=fulltext

[53] Nesbitt, Brian (ed.), *Pumping Manual International, Handbook of Pumps and Pumping*, Elsevier, Oxford, 2005, p. 266.

encouragement of high quality European privacy certification schemes remains the core priority. Complying with the standard may prove costly for the privacy seals industry; it might also not provide an enhanced benefit as compliance with the standard might not be immediately visible to stakeholders.

Role of different stakeholders

This section outlines the roles we anticipate different stakeholders will play:

- **European Commission**: informal consultation prior to issue of study or programming mandates, draft and issue of mandate(s).
- **EDPB:** consult with, and assist Commission in development of Guidelines for Mandate.
- **EU standardisation bodies**: acceptance of mandate, development and adoption of Standard. The EU standardisation bodies are tasked with the initial responsibility of ensuring the proper execution of the accepted mandates as well as the conformity of the (harmonised) standards or alternative standardisation deliverables adopted with the mandate and the directive concerned.
- **Privacy, data protection certification schemes:** compliance with the Standard (apply for certification).
- **EU-level body/other organisation identified in Option 3:** accredit privacy certification schemes (*alternative 1).*
- **National accreditation bodies:** evaluate and assess privacy certification schemes (*alternative 2).*

Implementation, process, indicative implementation schedule, milestones

The Commission could draw up a draft mandate through a process of consultation with a wide group of interested parties (national data protection authorities, privacy certification schemes, consumers, SMEs, relevant industry associations, etc.). Before being formally addressed to the ESOs, the mandate would be submitted to the Committee on Standards of the Regulation (EU) 1025/2012. The Commission could then, based on the results of the consultation, issue a study or programming mandate to the ESO's (or alternately a combination).
The Vademecum states,

> In the case of new legislation, it is not always essential to await its final adoption before issuing a mandate. However, a stable text must already be available in order to begin standardisation work. A mandate based on the "common position" makes it possible to save time as regards standardisation and even as regards the implementation of the legislation concerned. In some cases it may be useful to issue a mandate, and particularly a programming mandate, as early as the moment of the adoption of the draft directive by the Commission.[54]

The development of the Standards generally takes the following steps: proposal to develop an EN, acceptance of the proposal, drafting, enquiry (public comment at national level),[55] adoption, publication and review (every five years) which results in confirmation, modification, revision or withdrawal of the Standard. The Standard and supporting

[54] European Commission, *Vademecum*, op. cit., 2009.
[55] The EDPB could be invited to comment on the Standard at this stage.

documentation should be made available to the public free of charge (or for a very nominal fee).

Once the standards are developed, adopted and submitted to the Commission, the mandate is considered complete (however, mandates must not be regarded as closed, but as being "dormant"). The revision of a European standard to adapt it to technical progress (cf. the internal rules of CEN and CENELEC) must in principle, be regarded as having to be carried out under the terms of reference of the mandate in question.

A standardisation mandate can be drafted by the Commission in less than one year. However, standardisation mandates may take up to four years to be fully implemented. We, therefore estimate the timeframe for implementation of this option to be between 4-5 years.

Impacts on stakeholders

This section outlines the impact of the option on different stakeholders:

a. *Individuals:* The British Standards Institution (BSI) states that "All standards affect the public directly or indirectly, even though most are produced to serve the immediate needs of business and industry. Many, though, have a direct and beneficial impact on the general public".[56] The impact of this option might not be very visible at this level; however, if a technical standard for privacy certification schemes is adopted, it will prove beneficial in the long run to individuals, specifically those that chose to rely on schemes meeting that Standard. It will also trust and confidence not just in one country but in a more harmonised manner across the EU.
b. *Relying parties or users:* can derive some benefits from knowing that privacy certification schemes (i.e. those that subscribe to, or are certified as meeting that standard) meet a high, European standard.
c. *Existing privacy certification schemes:* will face competitive pressure to conform to the Standard which will codify and diffuse state of the art.
d. *Certified entities (entities subscribing to the Standard):* will gain competitive and reputational advantages. If the Standard imposes too many restrictions, it may harm innovation. The Standard will help certification schemes demonstrate more accurately that they meet the harmonised EU criteria and requirements for privacy certification; thus, it will improve their credibility.
e. *Standardisation bodies:* will be involved more actively in the process. Their expertise and experience can be harnessed to foster the goals of privacy and data protection. They will need to provide a high level of commitment to ensure the whole process is successful.
f. *Industry*: on the whole a harmonised standard for privacy certification schemes in the EU will enhance data protection and privacy standards.
g. *Internal Market*: The harmonised standard will benefit the Internal Market by ultimately, reducing costs and facilitating trade within the EU.
h. *European society*: It will improve harmonisation in the privacy certification sector; it will also help build trust and confidence.

[56] BSI, "How Standards Help Consumers". http://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/how-standards-help-consumers/

Evaluation and conclusion

This option presents a means to implement mechanisms and procedures that support the execution of the law successfully, in an area that is technically complex. This option, if properly undertaken has the potential create a more harmonised privacy certification within the EU. A harmonised EU standard for privacy certification schemes can help such schemes achieve their objectives (to assure privacy and personal data protection, build and enhance consumer trust and confidence, generate privacy accountability, resolve disputes etc.) more efficiently and optimally. The standard will provide a harmonious framework for privacy certification schemes in Europe.

One of the recommendations at the workshop on *Considering Options for an EU Privacy Seal* held on 8 April 2014 in Brussels (under the remit of the Study on EU Privacy Seals) was to implement a softer option prior to the issue of a full mandate on a harmonised Standard for privacy certification schemes. However, we acknowledge that this recommendation might has different implications for different stakeholders. For instance, individuals and relying parties may want the harmonised standard developed and implemented as soon as possible, while privacy certification schemes may want to drag the process out.

The Standard should be built on a robust foundation; it should take advantage of the state of the art in privacy certification. There should be a reasonable timeline for its implementation and application. The Standard should not create prohibitive costs.

Further, there are also the challenges to its adoption and use (given that it will most likely be voluntary). Appropriate incentives would need to support the adoption and use of the Standard. It is also essential to reiterate that the development and implementation of a standard for privacy certification schemes does not detract or dilute the role of data protection authorities.

5.1.5 (EU criteria-based) certification by national data protection authorities

This option envisages that while the criteria and requirements for the award of an EU privacy seal would be set centrally (presumably, either by the European Commission or the EDPB, once the GDPR comes into effect, or the Article 29 Data Protection Working Party until such time), the scheme itself would be run by Member State data protection authorities (DPAs). The DPAs could be involved in this process directly by certifying applicants, or indirectly by endorsing independent third party organisations to run the scheme on their behalf (as envisaged by the UK Information Commissioner's Office scheme).

As a preliminary remark, this option does not constitute a standalone solution as the substantial and organisational rules for an EU privacy seals scheme would have to be devised centrally at the EU level. National DPAs would only run the scheme without having the right to add or take away anything from it in their respective jurisdictions. Such central introduction of rules could therefore follow one or more of the options analysed in this report (encouraging and supporting the GDPR certification regime, creation of a harmonised standard, or full regulation).

Regardless of the specific method through which the central rules will be devised, they will have to deal with a number of important issues varying from strategic and planning matters (for instance, whether the seal 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, whether it will be based on formal EU legislation, i.e., a Regulation or a Directive, or on soft law, e.g., an EDPB opinion or a Recommendation, 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 involve important decisions that will determine, in essence, the nature of the EU privacy seal scheme. In the same context, as monitoring of the scheme and updating are central elements of a successful certification scheme as determined in Task 3 of the Study,[57] the central EU-level body that outlines the criteria and requirements would need to be involved in these tasks.

In view of the above, regardless of the actual criteria-setting mechanism (the Commission, the EDPB or other), the principles of transparency and participation are particularly relevant. For the scheme to resound with all stakeholders, the setting of the criteria and requirements should, as far as possible, be open and transparent, allowing for wide stakeholder involvement, public participation and scrutiny. We recommend the adoption of concrete measures to achieve this effect. It might also be better to separate the resolution of the issues related to the design of the certification mechanism, from the issues related to its administration at the national level.

The aforementioned broad partition of competencies is an important distinction of this policy option: the decision-making (criteria and requirements setting) for the scheme will be operationalised at the central level, and therefore common across the EU, while Member State DPAs will be responsible for running the scheme, assuming therefore a more or less an execution role.

Even with such strict boundaries, however, "running" an EU privacy seal scheme by Member State DPAs has several further possibilities: DPAs could run the scheme themselves, directly certifying applicants,[58] or they could outsource the certification to third parties they endorse. These third parties could be more than one, allowing thus for competition in the relevant market, or a single party per processing sector (or, even, for the whole Member State, allowing perhaps sub-contracting). A number of other questions about the same (third) parties could equally be raised, ranging from their legal status (public or private, for-profit or not) to their relationship with their customers, data subjects, competent DPAs and the EU decision-making body (which could be governed by contract, by law or even by *soft* law). An important issue is Member State flexibility on the above possibilities – i.e., whether each Member State DPA will be allocated enough decision-making power to choose freely which system to implement within its jurisdiction (inevitably leading to a multitude of implementations across the EU) or not.

Although the risks and uncertainties of this policy option are analysed below, under the standard criteria analysis that follows, two points merit special attention. The first pertains to a potential change of role for Member State DPAs. Under the data protection system in effect today in the EU, DPAs are independent state authorities that monitor the application of, and ensure respect for data protection legislation within their territories. This basic notion is not

[57] De Hert, et al, *Task 3*, op. cit., 2013.
[58] The GDPR (Parliament version) Article 39 (1) (d) proposes that "During the certification procedure, the supervisory authority may accredit specialised third party auditors to carry out the auditing of the controller or the processor on their behalf".

affected in the text of the proposed GDPR either. If Member State DPAs choose to award privacy 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 privacy 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 case, even under the best circumstances of transparency and rule of law, data subjects might view the double role of DPAs with suspicion. This might lead to a loss of public trust, an otherwise critical element for the success of a (privacy) seals scheme, as demonstrated in Task 3 of the Study.[59]

The second important challenge to be addressed by DPAs under this policy option is resource allocation. Over the past few years, DPAs have witnessed an increase in their workload, due to an increase in personal data processing and development of related technologies, without such increase being necessarily accompanied by an increase in their allocated (financial or other) resources. Their direct involvement in a new resource-hungry system that could potentially cover a wide variety of processing sectors that they otherwise control could prove disproportionate with regard to their actual capacity, particularly if they take on the core task of certifying data controllers directly. From this point of view, it is possible that a high-level approach to this policy option by DPAs, wherein they only control and monitor certifiers who would run the certification scheme, seems more feasible.

There are some 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. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Germany, used to run EuroPriSe till 2014, however the scheme has now been transferred to EuroPriSe GmbH, a private entity.[60] Both efforts, demonstrate there are some limitations of DPAs attempting to assume the role of certifier.[61] More recently, the UK Information Commissioner Office (ICO) announced a "co-regulatory approach to seals, whereby their office will produce an overarching document outlining what they would want from this scheme, however it would be left to industry to determine what elements would be assessed when certifying companies".[62] In addition, the UK ICO "would sponsor schemes in conjunction with a national accreditation board such as the UK Accreditation Service (UKAS)".[63]

In view of the above, without prejudice to the detailed analysis on the basis of common criteria for each policy option that follows, it appears that the sustainability of this policy option could be better served under current circumstances through the model of Member State

[59] De Hert, et al, *Task 3,* op. cit., 2013.
[60] See ULD, "EuroPriSe 2.0 – Continuation of the European Privacy Seal (EuroPriSe) by EuroPriSe GmbH – Extended range of certifications", 14 November 2013. https://www.european-privacy-seal.eu/ws/EPS-en/Press-releases
[61] Our analysis of the EuroPriSe scheme in Task 1 showed a lack of interest and low take-up. In the case of CNIL label, we found it had a delineated geographic boundary matching the remit of the organisation and there is a less incentive for a website or service provider outside these jurisdictions (or not intending to operate within them) to participate. Further as noted in the Task 3 report, despite certification, a product or service could be misused and risks could continue; there are also the difficulties involved in subsequent monitoring (especially in the European context.
[62] See Data Guidance, "UK: ICO to launch privacy seals scheme 'within the year'", *Privacy This Week,* 27 March 2014.http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2258.
[63] Ibid.

DPAs outsourcing the certification role to third parties while themselves retain their typical role of monitoring and controlling to guarantee an adequate level of data protection within their jurisdiction.

Context, applicability and scope

This policy option refers to the establishment of common EU-wide criteria for a privacy certification scheme based on which the scheme would be run in each Member State by, or at least, under the responsibility of the DPAs. While the criteria 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, Member State DPAs could still be left with substantial space for flexibility while implementing the scheme at the national level. Most importantly, Member State DPAs could choose whether they would themselves assume the role of certifier or whether they would outsource this task to a third party or parties.

This option should be compatible with the Commission's original version of the GDPR and the European Parliament's version. In its draft, the Commission suggested that "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" – Article 39 (1), while itself assuming the role of "further specifying the criteria and requirements for the data protection certification mechanisms" (para 2), with such specification even reaching the level of laying down "technical standards" (para 3). The European Parliament's approach generally agreed with the EU model but essentially changed the central decision-making mechanism (the EDPB rather than the Commission) and specifically referred to the needs of SME data controllers. Both iterations favour a policy option wherein common EU criteria are set, and subsequently applied at Member State level by national DPAs.

Inherent risks and uncertainties

This policy option requires a number of challenges to be addressed both at EU and Member State level. At the EU level, the central decision-making about the criteria, requirements, actual set up and operation of the scheme would profit from the principles of transparency and participation. As these strategic decisions will directly impact routine personal data processing at Member State level, affecting both data controllers and data subjects, public trust would be enhanced through possibly open, public and participatory processes. A decision-making process that is perceived as taking place behind closed doors would ultimately reduce the perception and use of the scheme by its recipients in the market.

At the EU central decision-making level, an important difficulty for this policy option is the requirement for constant maintenance and updating of the scheme's operational details. It will also be necessary to develop a transition solution for the existing privacy and data protection certification schemes developed in Member States. As a privacy and data protection certification scheme would necessarily follow personal data processing trends, and indeed in different sectors, a necessary condition for a successful and relevant scheme refers to its continuous monitoring and updating with accumulated expertise. This task might require the establishment of a permanent mechanism or, alternatively, could use up substantial resources of an already existing organisation. The level of expertise required should not be overlooked.

This option ultimately requires a flexible, adaptive EU mechanism that would be predominantly involved in the process of establishing and operating the scheme at a high level.

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 indeed supported by applicable legislation, as independent regulators of data controllers and provide assistance to data subjects in exercising their rights. Their actual and perceived independence is therefore essential in executing their duties. Their potential involvement in directly awarding privacy 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. 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 privacy and data protection certifiers. Practically, it may mean that activities and sectors that are controversial from a data protection perspective will not benefit from certification, or that a very high level of data protection will be required for such activities.

Similarly, the operation of a privacy 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. 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 themselves successfully.
Other risks at Member State level involve legal uncertainty, public awareness and sustainability. A level of legal uncertainty could be expected at least until the seal scheme is established; for an intermediate period data controllers, data subjects and possibly courts might struggle to deal with a new data protection tool aimed at facilitating quick assessment and public trust (especially if it needs proper placement within the legal system concerned). Public awareness, an otherwise crucial element for a successful privacy seals scheme, will be achieved only through an adequate deployment of substantial resources to this end, and could be hindered if at the EU level a decision is made to create a scheme that allows non-uniform naming and branding. Finally, important decisions would need to be made with regard to system sustainability: regardless of whether the scheme is run by DPAs themselves or outsourced to third parties, a financial policy will need to be devised to ensure the scheme's sustained existence. However, if diverging national policies are adopted within an otherwise EU scheme, it would face the risk of forum shopping due to financial (and even application) considerations.

Obstacles to implementation

A substantial obstacle for the adoption of this policy model refers to the requirement of extensive regulatory (or, at least, institutional) intervention prior to its launch. As described above, the first stage of implementation would involve important decision-making at the EU level. First, this involves option selection, detailed elaboration and setting of the common criteria and requirements for the establishment and operation of the EU privacy seals scheme. This process will be time-consuming, regardless whether undertaken by the Commission alone, by the EDPB or a different organisation. Some aspects may require very broad

consultation. 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 privacy seal scheme be launched.

The range of the options outlined above, the timing of the GDPR, as well as the possible delays that will result at national level, point to an EU privacy seals scheme that might take a substantial amount of time to establish and to implement. Although this is normal while setting up a new certification mechanism, personal data processing needs, at least when viewed from the data subjects' perspective, often require a quicker response. A model that will take years to be established might have to deal with new technological and data processing circumstances that could make that could make assumptions at its inception irrelevant.

Finally, the multitude of possibilities for Member State implementations described above, if ultimately afforded in their full range to Member State DPAs, could presumably lead to a multitude of privacy seal models among Member States. This development could promote forum shopping and fragmentation, failing thus to bring the harmonisation and critical mass effect much needed in the contemporary privacy seals field (as demonstrated in Task 3).

Role of different stakeholders

Under this policy option, the role of different stakeholders will be decided after all relevant strategic decisions have been made. For instance, depending on the organisation that will make central decisions for the EU privacy seal scheme, the roles of the European Commission, the EDPB or other organisation, will differ accordingly. The same is applicable at the Member State level. Depending on the actual drafting of the scheme's operational particulars within the Member State, the role of DPAs could range from awarding the seals themselves to issuing guidelines and monitoring endorsed third party organisations.

While these roles remain open, the principle of participation should not be overlooked. To reiterate, it is important that decision-making particularly at EU level in relation to the scheme is as open, transparent and inclusive as possible; this will generate stakeholder and public trust in the scheme. The same is also true at Member State level: regardless of the final form of the scheme, the targets of the scheme i.e. data controllers and their representative organisations, need to be, and feel that they are, part of the process. A privacy seal scheme aims at flexibility, specificity and standardisation; all these targets are better achieved if the parties concerned, specifically in this case data controllers, are well informed about the criteria and requirements.

Implementation, process, indicative implementation schedule, milestones

Under this policy option the new EU privacy seal scheme would preferably be implemented immediately after the new GDPR comes into effect, but it could also be launched under the current, Directive 95/46/EC regulatory framework if deemed necessary or useful – the Article 29 WP could start developing an opinion on privacy certification seals and marks. Admittedly, it is within the GDPR environment (assuming that either the European Commission or the European Parliament models are ultimately adopted) that an EU privacy

seals scheme would fit best since explicit provisions in the GDPR support its introduction, provide guidance on some particulars and a support mechanism. In addition, a new privacy seals scheme would presumably, also fit well with other novelties introduced by the GDPR, such as privacy by design, the principle of data portability etc. The beneficial effect for both data controllers and data subjects of an EU privacy seals scheme that would facilitate quick assessments of compliance with an otherwise complex text (the GDPR itself), thus creating legal certainty, ought not to be forgotten. In relation to the competent authority for issuing certification, companies and the DPAs could also benefit from the criteria laid down in the Regulation for the one stop shop.

Despite all the above, an EU privacy seals scheme could presumably be initiated and become operational also under the current Directive 95/46/EC regime. Although no reference to such a scheme is found in its text, nor is a relevant legal mandate present (neither is there an express legal provision forbidding it), it could be initiated and run at the EU level by the Commission or another EU-level organisation under current circumstances; thus if this path is taken, there appears no legal obstacle. In this case, decision-making about the scheme would have to cover broader issues due to the lack of formal guidance, but any relevant initiative should involve wide public consultation and participation and should take into account the findings and results of this Study.

The process through which such an EU privacy seals scheme could be introduced is self-explanatory under this policy option: first, decisions need to be made at the central, EU level and then each Member State, presumably the DPA or other law-making body would implement the model within its jurisdiction. In essence, the process of implementation is a top-down process, rather than the opposite. Within this process, the broad milestones include specification of the regulatory and operational framework by the EU-level body and, second, adoption of the scheme at the Member State level and notification to the EU-level body that its scheme has become operational and providing details on its particulars. As the scheme is based on guidance at the EU level, the drafting of those documents could be relatively quick, building on the assumption that a consensus would be found on the broad requirements at national level. However, implementing the scheme at national level may depend on support from national government to provide the necessary means to DPAS, and possibly also from legal adaptations at national level.

We estimate the timeframe for implementation of this option to be around 5 years.

Impact on stakeholders

This section outlines the impacts of this option on relevant stakeholders.

a) *Individuals:* Under this policy option, given DPAs will be directly or indirectly involved, the protection afforded to individuals will be of high level. Regardless whether DPAs assume the role of certifiers or endorse third party organisations to run the scheme on their behalf, at Member State level it will be the DPA that will constitute the competent authority overseeing the scheme. Consequently, data subjects will continue to have a focal point, their local DPA, when seeking assistance to enforce their data protection rights. Having the same contact point for certification related issues and compliance issues may ease the interference between individuals and DPAs. However, the aforementioned risk of a, presumed or true, conflict of interest must not be forgotten. If DPAs assume the role of certifiers themselves,

individuals may feel that DPAs have compromised their role as guardians of their data protection rights within their respective jurisdiction. This is a serious risk that ought to be weighted carefully by Member State DPAs when deciding which certification model to implement.

b) *Relying parties or users:* The implementation of any EU privacy seals scheme seeks to achieve an increased level of trust and confidence, per its declared objectives (in the relevant legal provisions). Although such a comparison would be difficult to construct, 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 (see above under *impact on individuals*), will vary depending on the actual model implemented within each Member State. In essence, the level of trust might vary depending on whether the scheme is directly run by DPAs or whether it is outsourced to third parties. If DPAs assume directly the role of certifiers, the underlying conflict of interest might adversely affect public trust and confidence in the overall scheme.

c) *Existing privacy certification schemes:* Under this option, existing certification schemes will continue to exist. In Tasks 1 and 3 of the Study, we noted that these 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 criteria and requirements to bring it in line with the EU-level criteria and requirements. If national DPAs decide to outsource certification, they might endorse some of the existing privacy certification schemes that meet the criteria and thus their role would continue (with the advantage of being able to harness their knowledge and expertise) under the new regime. However, if the local DPA decides to undertake the certification task itself, existing scheme operators might face competition and some of the schemes might become obsolete.

d) *Certified entities or scheme subscribers:* From the scheme subscribers' or certified entities' perspective, any successful EU privacy seals scheme would, among others, enhance their market reputation and credibility, create legal certainty and enhance the maturity of their data protection management systems.

e) *Standardisation and certification bodies:* EU standardisation bodies might have a role to play in this option, if for example, as outlined in option 4, they contribute to a harmonised European standard or family of standards for privacy certification schemes through the European standardisation (EN) framework, or they are involved as relevant stakeholders in a EU level consultation on the criteria and requirements for the scheme. Alternately, they might not be affected at all, depending on the actual model of implementation.

f) *Industry:* Any privacy seals 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. If DPAs outsource the certification work to third parties, industry associations might assume this role, bringing, thus, the necessary flexibility and expertise required for the operation of a successful privacy seals scheme.

g) *Internal Market:* 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. It is possible that national implementations differ as much as DPAs assuming the certification role themselves to

DPAs outsourcing the task to third parties or DPAs awarding relevant certification contract to multiple parties within their jurisdiction, creating thus a market. If this happens, the harmonisation effect that constitutes an important priority for an EU privacy seals scheme (as outlined in Task 3), would probably not reach the level intended: 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 as the seals scheme branding (a common EU label 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.

h) *European society:* An EU privacy seals scheme would facilitate the exercise of data protection rights by data subjects, and create increased legal certainty to data controllers. The involvement of Member State DPAs in the scheme, regardless of their exact role, warrants a possibly high level of attaining the above objectives, while at the same time benefiting European society.
i) *Regulators and policy makers:* Regulators and policy makers might be involved under this policy option at two stages: first, in drafting the common criteria for the EU privacy seals 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 co-ordinated actions and informed choices that would benefit not only broader data protection purposes, but also result in an effective and sustainable EU privacy seals scheme.
j) *International community:* 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 foresee the international impact this option would have on the 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 addition of the EU data protection model or not.

Evaluation and conclusion

This option envisages that while the criteria for award of an EU privacy seal would be set centrally and the scheme would be controlled by Member State DPAs who would either be involved in this process directly or indirectly by endorsing third party organisations to run the scheme on their behalf. There are different permutations possible under this option. The above distinctions illustrate the multitude of options while implementing this type of an EU privacy seal scheme. The final format of a scheme developed under this option will affect its performance in practice. However, even at a conceptual level, a number of issues can be highlighted in relation to it:

- The scheme will benefit more from an application of the principles of transparency and participation both at the drafting and implementation stages;
- To achieve harmonisation and integration within the internal market a number of significant decisions need to be made, i.e., that the criteria for the scheme will be

common for all EU Member States and DPAs will be free to choose within a limited, range of local implementation options and common approaches will be required as regards enforcement of the certification, allowing cross border enforcement in case of issues, building on the consistency mechanisms foreseen in the Regulation;

- The most important risk for this policy option is a real or perceived, conflict of interest for DPAs. If they run the scheme themselves within their respective jurisdiction, they might face real or perceived difficulties in controlling data controllers certified by them;
- DPAs will require substantial resources to run a seal scheme (ideally, for many different processing sectors) themselves;
- For the above two reasons, it might be advisable for DPAs to outsource the certification work to qualified third parties (either one or many) within their respective jurisdictions;
- An increased level of flexibility, to accommodate local particularities, is justified through this policy option;
- Legal certainty will depend on the central decision-making and could be hindered during the early stages of implementation due to localisation of the scheme by DPAs;
- While Member State data controllers will profit from involvement of their respective DPAs, international data controllers might find the scheme, particularly during its early stages of implementation, not suited to their particular needs and controller may wonder whether a certification awarded by a particular national DPA or even regional DPA, as could be the case in Germany, will have a sufficient echo at EU level.

Despite these issues, the involvement of DPAs in the EU privacy seals scheme (whether directly or indirectly will boost public trust and confidence and allay many of the concerns evidenced in the current self-regulated privacy seals sector.

5.1.6 Full regulation (further extension of Article 39)

This policy option envisages a full regulatory approach to EU privacy seals. Under such a scheme, all decisions will be taken at EU level, through the GDPR text and subsequently by means of specific legislation (such as a specific legal proposal or if rendered possible by the co-legislators, delegated acts and technical standards). Consequently, the main decision-making regarding the "criteria and requirements" for the scheme itself, the "conditions for granting and withdrawal", the "requirements for recognition within the Union and third countries", their "technical standards" and the introduction of "mechanisms to promote and recognise certification mechanisms and data protection seals and marks"[64] will all be defined centrally, following a proposition from the European Commission that should be approved by the co-legislators, for all Member States. The latter will presumably assume an auxiliary role, ensuring the proper implementation of the scheme within their national borders.

A couple of clarifications are necessary to properly place this option among the other options examined in this report. Full regulation may be articulated within other options as well, for instance in the option on (EU criteria-based) certification by national data protection authorities discussed in 5.1.5, if what is ultimately devised in practice is a model wherein EU decisions are made by a formal body (the Commission, or the EDPB if granted regulatory powers) and Member State DPAs regulate the field in their respective jurisdictions, either alone or in co-operation with law-makers of the state concerned. In this case, scheme

[64] See Articles 39 (2) and (3) of the original European Commission proposal.

participants would be faced with a formal, fully regulated seals scheme, despite its origins. This option covers a scenario where decision-makers and other stakeholders intentionally choose to construct a fully-regulated scheme that will leave no space for derogations, disharmonised approaches or divergent implementations at the Member State or end user level. Although this could take place under other policy options too, in essence this policy option refers to the intention of decision-makers not to leave the final outcome open to circumstances and the conditions in the market or the Member State level.

This option widely differs from the option outlined in section 5.1.1 (Encouraging and supporting the GDPR certification regime). While policy option 5.1.1 envisages the European Commission encouraging the Article 39 certification mechanisms through soft measures, this policy option envisages a more determined approach by the Commission whereby it issues formal measures to introduce and operate an equally formal privacy seals scheme across the EU, varying thus qualitatively its level of "encouragement" for the establishment and participation in such certification mechanisms.

A second, vital clarification is that the model discussed in this policy option expressly relates to, and intends to provide additional measures to the ones foreseen in Article 39 of the original European Commission GDPR proposal. This is done to set a common basis of understanding. Though a fully regulated model could take many forms - the one this report analyses, refers to a Regulation-set model, where subordinate technical legislation sets the scheme details. Alternatively, a fully-regulated model could be derived by introducing a standard-setting, detailed Directive relating to the scheme and subordinate, technical legislation supporting it, or even a series of subject-matter specific (meaning, seal-dedicated) Directives each regulating, for instance, different personal data processing sectors. The same would probably be the case if legislators decided to use Framework Decisions to achieve this objective.

In essence, full regulation may come in as many forms as the number of regulatory tools available in EU law. This multitude was partially made visible in Task 2 of this Study, where we examined different implementations of established EU certification schemes (and, therefore, their supporting legal regimes) in different sectors. A choice had to be made in elaborating this policy option: first, to create a common basis of understanding and reference and, second, to make this task feasible (since any attempt to analyse all of the above different law-making options would require a separate, dedicated analysis). Article 39 of the original Commission's draft of the GDPR appears to be a reasonable choice given, first, preference to it at least by the European Commission who drafted it and, second, it presents a well-thought and workable option, at least if this option was ultimately agreed by all the parties involved (the Commission, the Council and the Parliament).

The final clarification is that the above three bodies (the Commission, the Council and the Parliament) need to agree upon the final wording of Article 39 and related certification provisions, before work on the option suggested here can be concretized. As will be immediately analysed, Article 39 includes a structured, workable model of full regulation for the introduction of an EU privacy seals scheme. As expected, this model has its theoretical and practical premises, conditions and planning. If part of them goes missing, then the model will cease to be workable, at least as intended by its authors. This also means that the model will lose its character, and will consequently cease to be a prototype for a fully regulated model.

In view of the above, the following analysis aims at elaborating the risks and benefits of implementing a full regulation approach for an EU privacy seals scheme. The analysis will use as a basis of reference the model of Article 39 outlined in the original European Commission GDPR proposal, which is essentially one of many within the same category. Where possible this distinction will be made explicit in the text that follows (accordingly, unless this is expressly done, whenever full regulation is referred to, Article 39 is used as basis of reference). This option considers that Article 39 lays down the basis for a fully EU level regulated EU privacy seal.

Context, applicability and scope

This option envisages a full regulation model for an EU privacy seal scheme constructed at the EU level, through appropriate regulatory acts issued by the Commission. The various actors and participants in the certification process (certifiers, accreditors, data controllers and certified parties) would merely have to apply the rules and regulations prescribed in EU regulatory texts. From a conceptual point of view this policy option presents two undeniable benefits: simplicity of concept and applicability. As far as the former is concerned, an EU privacy seals scheme introduced and operated centrally for all EU, either by the Commission or by a dedicated mechanism, either new or already established, represents a simple concept that has appeal not only for data controllers but also data subjects. It is worth noting that, the same concept has been used in other fields (see the analysis of Task 2 of the Study, for instance the CE marking scheme) and consequently both end-users and scheme participants are accustomed to similar initiatives undertaken by EU institutions. The application of this policy option depends on its nature: a lack of or minimal stakeholder and Member State participation in setting up the scheme might lead to complex legal models and implementations, direct EU regulatory intervention essentially means that the scheme will be up and running immediately after the relevant acts have been issued without any need for further localisation and customisation.

A centrally run, fully-regulated EU privacy seals scheme that would complement an otherwise equally fully-regulated EU general data protection model would probably constitute an expected solution to achieve the overarching goal of harmonisation pursued by the EU. Harmonisation for privacy seals in the EU would be best served through a full regulation model (by a Regulation) and not multiple local models (under a Directive).

The method of implementation is of importance even within the strict limits of a full regulation model. The model under examination (Article 39 of the GDPR) places a Regulation at its basis where the general priorities are set ("allowing data subjects to quickly assess the level of data protection provided", "proper application of this Regulation, taking into account specific features") while leaving it to delegated acts and technical standards to undertake the rest of the required operational details. This constitutes a complete, at least conceptually, and hierarchical seal scheme model. It is also aligned to the GDPR general expectation for it to constitute the basic text of reference with regard to EU data protection. This option presents, therefore, an increased level of compatibility with the broader GDPR model, in the sense that the GDPR intends to replace national data protection acts and constitute the basic EU regulatory data protection text. As already analysed, full regulation could be accomplished in other ways too – however, it is doubtful whether any other policy option within the same category would present the same level of compatibility and complementarity to general GPPR purposes as the model described in Article 39.

Inherent risks and uncertainties

The inherent risks and uncertainties involved in this option mostly pertain to difficulties related to any regulatory model designed and implemented through a top-down approach: namely, inflexibility towards its recipients and participants, disregard of local particularities, lack of participation and transparency, as well as, limitations in scope and/or diffusion potential given the inevitable restricted resources. In addition, a broader uncertainty refers to the final wording of the GDPR in this regard, in the sense that Article 39 prescribes a structured and complete certification system that, if affected through the forthcoming *trialogue* or otherwise, might cease to fulfil these criteria. This can be alleviated by implementing other options such as option 1 in parallel or in preparation to this option.

An EU privacy seals scheme would ideally present an increased level of flexibility to address the particular needs of specific processing sectors. Such flexibility may certainly occur once the scheme becomes operational and take place at local, Member State level, however it can also, and would probably be preferable if indeed this was the case, occur while drafting the scheme. Sector-specific regulations, that would make the general provisions of the GDPR concrete to the processing details of any given industry, would most benefit both the data protection purposes and the scheme itself. Participants would see clear benefits in adopting a scheme especially designed for them and tailored to their needs. The Article 39 approach, whereby the Commission will lay down technical standards and delegated acts hardly accommodates any of the above. From this point of view it could even be said that Article 39 leads to a self-contradiction, given its paragraph 1 requirement for certification mechanisms to "take account of the specific features of the various sectors and different processing operations" while at the same time not affording its lead authority (the Commission) with the tools to achieve this goal. Any seal scheme expected to be designed to its last detail by a central authority, even if it incorporates best practices of public consultation and public access to policy documents, is bound to be (at least compared to other policy options presented in this report) less flexible and specific to the processing it purports to certify.

In the same context, an EU privacy seal scheme designed by the Commission alone as prescribed in Article 39 of the GDPR risks ignoring important local, Member State peculiarities. Although this might be an intended risk, outweighed by the important benefit of achieving harmonisation and internal market integration, local peculiarities could affect such a scheme's performance in practice. As shown in Task 1, the approach among Member States to privacy seals varies substantially: while some of them have experimented extensively or are even rigorously with privacy certification schemes, others have no experience in this field. Even among those active in the field, approaches vary considerably, ranging from full-fledged DPA involvement to a market, self-regulatory approach. A fully regulated EU privacy seals scheme that would replace all of the above with a new mechanism designed in its last detail to become operational immediately risks hitting against the above two-speed (or even, multiple-speed) approaches in place today, and therefore creating confusion, uncertainty and conflicts. Local rules and practices may have to be abolished (the legal effect of such abolishment would not be straightforward in all Member States) and new ones will have to be established that could perhaps overlap or conflict with neighboring legal rules. Member State implementation of a fully regulated EU privacy seal scheme is not a straightforward process, and will require time and resources to become seamlessly integrated and fully serve its purposes.

Building a privacy certification system based on legislation takes times, even if the procedures related to delegating and implementing acts may be significantly shorter than

when a fully new proposal is tabled by the Commission. The creation of such regulatory texts is not an easy task, as the Commission, applying its best practices for these purposes, will need to include in the process relevant stakeholders by conducting public consultations, assigning research reports etc. Even with the best intentions and resource support provided by the Commission, this process cannot simultaneously take place for a great number of processing sectors. Output will inevitably need to be prioritised and organised in a rational manner. This is an inevitable limitation of any top-down regulatory approach. In this way, however, though it might be a good starting point and while certain processing sectors will benefit from introduction of an EU-wide system and accompanying customised rules, others will be inevitably be left behind. Data controllers and data subjects involved in the uncovered sectors might, consequently, see little benefit by the introduction of an EU privacy seals scheme that would be, in practice, may not addressed to them in a first stage. Although this difficulty is effectively an early-adoption problem that can be addressed over time, this required longer period of time creates uncertainties particularly given the GDPR timing (in effect, to become effective within a couple of years at the earliest), and that personal data processing is increasing at an exponential rate and will not decrease in the foreseeable future.

Finally, a broader uncertainty relates to the ultimate wording of the GDPR if a full regulated model is adopted. Article 39 prescribes some guidance for setting up a fully regulated EU privacy certification mechanism. However, if the final wording of this Article changes its current format, the model prescribed here may change, potentially affecting the benefits it presents.

Obstacles to implementation

Potential obstacles to the implementation of a fully regulated EU privacy seals scheme along the lines of Article 39 of the GDPR include: complexity of the drafting exercise, the requirement for a permanent monitoring and update mechanism, possible application difficulties at Member State level, as well as, financial sustainability of the scheme, and the duration of the legal process necessary for it to enter into force.

With regard to the complexity of the drafting task, the design, introduction and application of a fully-regulated EU privacy seals scheme will constitute a particularly demanding exercise for the organisation that will undertake it (in this case, the European Commission). The level of detail that a workable privacy seals scheme will need to attain means that its drafters will have to fully-acquainted with the particularities and details of any processing sector which the scheme will aim to regulate. Given the general GDPR ambition for the scheme to cover as many processing sectors as possible to adequately serve its purpose, this exercise will have to be repeated for each of them. The resulting workload will be substantial – and complex. Such demanding requirements for the release of sector-specific seals might ultimately constitute an important obstacle to their possibly widespread implementation.

Another obstacle to its implementation refers to the need for an EU privacy seals scheme to be monitored, updated and operated by a permanent, central mechanism. The need for constant monitoring of the scheme's operation and the frequent updates will include (broadly following the pace of technology and processing practices) make the establishment of a permanent mechanism that will undertake these tasks centrally important to its success (also evidenced in Task 2). However, the creation of a new, dedicated mechanism may not prove a simple task within formal EU infrastructure.

Obstacles to implementation of an EU privacy seals scheme might also appear in the form of local, Member State peculiarities that affect the application of the scheme within their respective jurisdiction. This risk has been outlined above; here it is sufficient to note that a fully regulated, centrally designed scheme, such as the one prescribed by Article 39 of the GDPR, might contrast with established rules and practices at Member State level that will at best need time to raise and at worst make the scheme irrelevant to the participants concerned.

Finally, an EU privacy seals scheme needs to be sustainable. Financial resources come in many forms, for instance, EU funds, participant fees, Member State support etc. In this context, it is possible that a fully regulated (by the European Commission) model might prove incompatible with some of these resources (for instance, direct Member State support) or might unduly burden the EU budget. The legislation underpinning the scheme will have to specify who will be responsible for collecting participant fees and constructing the relevant financial mechanism. These are important questions that need to be addressed and resolved.

Role of different stakeholders

The role of different stakeholders is expected to be limited under this policy option. Within a fully regulated model, we envisage it is the primarily the body concerned (in this case, the European Commission) that will hold the central, if not exclusive, role in the process. This body will draft and release the rules, monitor the operation of the scheme and update the model, when required. The role of other stakeholders (DPAs, other Member State agencies, national regulators, standards operators etc.) may be of an auxiliary nature, depending the final form of the scheme. Such roles could include anything from data controller certification, certification renewals, scheme "localisation" into Member State infrastructure, fee processing and collection or even some form of market surveillance. Stakeholder involvement could include participation in European Commission consultations on the criteria and requirements and the technical standards. However, a fully regulated model does not encourage the partition of substantial roles among many stakeholders as the majority of the decision-making is vested in a single, organising body.

Implementation, process, indicative implementation schedule, milestones

A fully regulated EU privacy seals model designed along the lines discussed in this policy option presumably has a fairly straightforward implementation schedule and consequently a limited number of milestones. Given the authority of a single body to design and implement the scheme, the important milestone, once the GDPR and specifically, Article 39 come into effect, is the issue of the delegated acts. These may be cross-sector or sector-specific, depending on the plan of the implementing organisation (the European Commission). Milestones also include the technical standards that will supposedly follow the introduction of the delegated acts and are most likely to complement them in sector-specific processing.

Once the EU privacy seals scheme becomes effective, Member State implementation efforts shall follow. This could take many forms and progress at different paces: Member States with prior experience in the field and/or whose legal systems and local practices are not in conflict with the new scheme's details are most likely to take full advantage of it first. Where there are obstacles (such as those outlined before), implementation might follow at a slower pace. The level of sophistication of the digital and information technology sector and penetration in general, is also relevant and might affect implementation. Therefore, milestones at this stage

refer to each Member State's response to the certification scheme and its success in implementing the scheme within its jurisdiction.

We estimate the timeframe for implementation of this option to be around 5 years.

Impact on stakeholders

This section outlines the impact of this option on the relevant stakeholders.

a) *Individuals:* A fully regulated EU privacy seal scheme, expressly created according to its legislative mandate will help individuals quickly assess the level of protection afforded by data controllers, and generally, these individuals will benefit from a high level of data protection. Given the specificity of some of the provisions on certification mechanisms and seals in the GDPR, the European Commission is expected to release a scheme that places the data protection purposes as its priority. In doing this, it will benefit from the new regime of the regulation as to some practical issues: e.g. the means of dispute resolution, individual redress, and applicable jurisdiction (even among Member States), nevertheless further specification of the regulation as regards these issues will need to be dealt with. The data protection purposes, at least from a data subject's perspective, may only be realised if adequate answers are provided to the above questions, affording individuals with an effective system for the protection of their rights.
b) *Relying parties or users:* Public trust and confidence is perhaps best realised by a fully regulated certification mechanism in comparison to other (self- or even co-regulated) policy options. Although no measurable evidence exist to justify this statement, past experiences with regard to self-regulated schemes points to little public trust in them.[65] As shown in Task 1, DPA operated schemes generally scored better than privately run schemes against the GDPR criteria analysis.[66] In addition, the examples of EU certification in other fields, as analysed under Task 2 of this Study, generally showcase successful seal systems that enjoy wide recognition in their respective fields. Given the above, we expect a fully regulated EU-initiated and run system will be perceived in a positive manner by its intended users and ultimately lead to wide use and acceptance.
c) *Existing privacy certification schemes:* Existing privacy certification schemes will have to compete with a fully regulated EU privacy seal scheme, and there is a need to identify further their role within an integrated across the EU environment built upon the new model.
d) *Certified entities or scheme subscribers:* A fully regulated EU privacy seals scheme that will be planned and operated centrally, will benefit primarily subscribers operating across the EU. A uniform system with common rules and characteristics across the EU will create legal certainty and cost minimisation for entities that are active in more than one Member States and wish to be certified. This will strengthen one of the core objectives of the GDPR - to create a possibly harmonised data protection environment across the EU. On the other hand, entities that are active only in a single Member State may not see practical benefits in participating in such a scheme compared to using a national scheme.

[65] Rodrigues et al, *Inventory,* op. cit., 2013.
[66] Ibid.

Apart from practical issues, however, a fully regulated EU privacy certification scheme is expected, as seen above, to score better in matters of public trust and confidence. If compared to local implementations (even if DPAs are involved in the process), a central scheme, common for all the EU, initiated and controlled by the Commission could achieve better public recognition and, if no application problems occur, an increased level of public trust. Such public trust and confidence will benefit all scheme subscribers, regardless whether it operates locally or across Member State borders, balancing therefore the above finding that a fully regulated model would primarily benefit the larger (international) data controllers. Finally, Article 39 of the GDPR, expressly refers both to data controllers and to data processors. This is an important distinction particularly relevant to the cloud computing environment where cloud operators are frequently found to be *processors* rather than *controllers* of the personal information they process, especially in a B2B service context.[67] In this context, the Cloud Computing Strategy refers to the need to produce the guidance on how to apply the existing GDPR, notably to identify and distinguish the data protection rights and obligations of data controllers and processors for cloud service providers, or actors in the cloud computing value chain.[68] Although the specifics of this discussion are beyond the scope of this analysis, an EU privacy seal ought to encompass all personal data processing instances regardless of their naming, and this priority is well identified, and covered, in Article 39 of the GDPR.

e) *Standardisation and certification bodies:* Under this option, existing standardisation and certification bodies might need to align their practices to conform to the new requirements. A fully regulated EU privacy seal model does not necessarily mean that existing standards or certification organisations in existence become obsolete. On the contrary, their gathered experience and expertise in the field could be put in use while certifying data controllers under the requirements of the new certification mechanism. A continued existence in parallel between the two should also not be excluded. The same is applicable with regard to standardisation bodies as well. Any already issued standards that will not be compatible with the new EU requirements will evidently have to be replaced, however, as the GDPR asks for technical standards to be issued by the Commission, this does not preclude standardisation organisations from issuing (voluntary) standards of their own neither does it keep them from consulting the Commission while finalising its own.

f) *Industry:* A fully regulated EU privacy seals model will impact the overall industry in a two-fold manner: it might lead to an increased level of data protection and legal certainty; at the same time, however, this model might involve a more demanding process for certification than other policy options. With regard to the former, a fully regulated EU privacy seals scheme, once it becomes applicable in the industry concerned (see the analysis above on risks and uncertainties), might create an integrated and harmonised certification environment across the EU that will warrant legal certainty particularly for international data controllers. In addition, as rules are set in detail by a central authority, this means not only that these rules conform to data

[67] See Poullet, Y., J-M. Van Gyseghem, J-P. Moiny, J. Gerard, & C. Gayrel, "Data Protection in the Clouds", in Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Springer 2011, pp. 377-409 [p. 386].

[68] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe COM(2012) 529 final, Brussels, 27 September 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

protection norms and principles but also ensure that a high level of data protection is assured. On the other hand, it is probable that the task of certification in such a scheme will be more demanding than in other policy options: not only will it need to be implemented at Member State level after central rules have been released but, as explained before, it might also be more inflexible and less accommodating to local peculiarities than other alternatives.

g) *Internal Market:* The Internal Market might benefit substantially from a fully regulated EU privacy seals scheme, because this policy option is more likely than any other to lead to the establishment of a strong, recognisable, pan-EU certification system that will be directly accessible and usable in all Member States.
h) *European society:* While its effectiveness with regard to its purposes will have to be tested in practice once released, a fully regulated EU privacy seals scheme will achieve public trust and confidence at a higher level than other policy alternatives. This in turn would benefit European society, in the sense that the data protection purposes (and the corresponding fundamental human right) will be furthered.
i) *Regulators and policy makers:* A fully regulated EU privacy seals scheme will possibly rely heavily on the work of regulators and policy-makers, at least at EU level (i.e. the European Commission, as per Article 39 of the GDPR). This could be challenging considering the need for a widespread, multiple processing sector scheme implementation. In practice, this could also prove an important difficulty for widespread, multiple processing sector scheme implementation, as explained above. Such a scheme might prove difficult and resource-demanding to manage and keep in operation (update, maintain and expand) across the EU in all personal data processing sectors. The details of sector-specific processing and Member State particularities are expected to be followed and accommodated with difficulty by a central law-making authority.
j) *International community*: Given that the EU data protection model is followed in several, but not all, countries outside the EU, a fully regulated model might be applicable only to those countries whose national legislation follows general EU data protection pattern. In such cases a successful EU seal scheme model is highly likely to become an exportable model.

Evaluation and conclusion

This option analysed the potential of full regulation approach to an EU privacy seals scheme. While recognising that full regulation might come in many forms, it has its advantages: for example, it scores well with regard to harmonisation and internal market integration, given its top-down, centralised approach, greater capacity to generate public trust and confidence, and an increased level of legal certainty. However, some concerns remain. This option is too prescriptive, inflexible and might lead to discrimination, at least in comparison to the other policy options, and this might affect its application at Member State level. This option also requires a significant law-making effort; making it sector-specific will also require significant resources that, unless dedicated to this task on a permanent basis, will hinder its further development.

6 ASSESSING THE IMPACTS AND COSTS OF THE DIFFERENT POLICY OPTIONS

This section presents a very preliminary analysis of the impacts and costs of the options analysed in section 5. This is an indicative, descriptive analysis, i.e., identifying some of the

impacts and costs of the different options, within the allotted scope of the study. We recognise that a perfect evaluation of all present and future impacts and costs of the options is a difficult task; the analysis outlined here presents the best possible conclusions based on the research conducted by the Study team in the preceding tasks, their expertise and the feedback from the Study workshop.

The analysis of impacts follows the stakeholders identified in Section 4 of this report. It is important to emphasise that the impacts on these stakeholders concern the specific issue of personal data and privacy protection (PD&P) in the context of the implementation of an EU privacy seal scheme. The generic impacts of personal data and privacy protection on these groups have not been considered. The different general functions of these stakeholder groups have not been considered, but only their stake in personal data and privacy protection.

For each option, different impacts with a brief description are outlined for each stakeholder group. Two different scales are used to assess the impacts and costs relevant to each option. It is important to highlight that there is often a direct or indirect proportionality between impacts and costs: for example, a full scale, EU-wide privacy seal will reduce existing fragmentation, but the associated coordination and policy making cost is, correspondingly, high. However, if poorly executed, even potentially low-cost options may result in higher costs.

At this stage, we need to emphasise that the assessment of impacts and costs of the six policy options poses several challenges due to the lack of availability of large-scale information and data on the specific impacts and costs of each policy option. Also, the schedules of implementation of the options might be highly different. The estimation of impacts depends on the potential selection and implementation of the policy option and its permutation, which in turn, is bound to its complexity and its diffusion across the EU. The empirical research did not specifically find "hard" data on costs relating to the creation, and operation of privacy seal schemes or policy options of similar nature, which again posed a challenge to the following analysis. For this reason we use two symbolic scales (shown in Table 1), one illustrating potential impacts and the other illustrating potential cost levels.

Impacts					
Scale of impact	**Not assessable**	**Neutral**	**Positive**		
	NA	**0**	**+**	**++**	**+++**
			Negative		
			-	**- -**	**- - -**

Costs					
Level of costs	**Not assessable**	**Low**	**Medium**	**High**	**Very High**
	NA	●	● ●	● ● ●	● ● ● ●

Table 1 Scales of impact and costs

Impacts can be positive '+' or negative '-'. The assessment estimates the probable level of impact by selecting one, two, or three symbols (e.g. a high positive impact is denoted by +++, a neutral impact by 0 and a mid-range negative impact by --. A non-assessable impact is denoted by letters 'NA'. Any signs in brackets e.g. (+) or (-) indicate an additional potential impact depending on the form the option takes based on policy and resource decisions.

Cost levels are indicated either as 'NA' (not assessable), and four other levels symbolised by bullets, with ● signifying low, ● ● indicating medium, ● ● ● indicating high and

●●●● indicating very high costs. Some costs are indicated with a (●), this denotes a potential additional cost depending on the form the option takes based on policy and resource decisions.

The following caveats apply to the analysis that follows:

1. The estimates of impacts and costs, although merely approximations, are still related to the actual impacts and costs of each option; thus, they do provide a realistic view on the prospective scenario that might apply to each option.
2. Each option carries within itself the possibility of mutating into different forms – this has implications not only for the impacts but also for the cost levels and the timescales.
3. Choices about what types or levels of measures adopted within the options, such as redress mechanisms and procedures, use of seal or logo, might lead to very different impacts and costs, than those outlined in this analysis.
4. An impact or cost might produce variant effects on the different stakeholders.

The implementation of each policy option might entail divergent types of policy-making effort and timeframes. Based on our research, the following table presents indicative timeframes for implementing each option.

Options	Estimated time frame
Option 1 Encouraging and supporting the GDPR certification regime	1-2 years
Option 2 Incorporation of EU data protection requirements into an existing EU certification scheme	2-3 years
Option 3 Accreditation of certifiers by an EU-level body	3-4 years
Option 4 Creation of a harmonised standard for EU privacy seals	4-5 years
Option 5 (EU criteria-based) certification by national data protection authorities	5 years
Option 6 Full regulation (further extension of Article 39)	5 years

Table 2 Options and timeframes

Note: The impact and costs tables that follow embed the time dimension in the scale of costs, i.e., the costs of implementing an option is not only estimated in terms of the effort needed for its full implementation but also embeds the time dimension.

6.1 ENCOURAGING AND SUPPORTING THE GDPR CERTIFICATION REGIME

As outlined in section 5.1.1, this option envisages the Commission using various soft measures to stimulate and encourage compliance with the GDPR regime for certification and seals. The table below outlines the impacts and costs for this option:

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
Individuals	- Easily and reliably verify PD&P rules respect and commitments	+	- Nil (assuming individuals, data subjects, or relying parties will not have to	
	- Improved trust and confidence	+		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	- Improved PD&P awareness	+	bear any costs specifically related to the scheme).	
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+		
	- Support to decision making on products and services in relation to protection of PD&P	+		
	- Easier protection of the data subject, (consumer) rights, provision of means and facilitation of disputes redress	++		
Relying parties or users (e.g., trust and confidence in organisations, products and services)	- Easily and reliably verify PD&P rules respect and commitments	+	- Nil (assuming individuals, data subjects, or relying parties will not have to bear any costs specifically related to the scheme).	
	- Improved trust and confidence	+		
	- Improved PD&P awareness	+		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+		
	- Support the decision making on products and services in relation to the protection of PD&P	+		
	- Easier protection of the data subject, (consumer) rights, provision of means and facilitation of disputes redress	+		
Existing privacy certification schemes	- Adherence to improved PD&P standards and good practices	NA	- Update and integrate certification schemes to comply with the EU seal scheme	●●
	- Improved accountability and enhanced trust and confidence	+	- Accreditation cost	●●
	- Improved market standing in relation to seal purchasers related to the certified PD&P processes	+	- Additional costs of scheme maintenance and operation, including regulatory approval costs and human resources and training costs	●●
	- Additional burden to comply with EU scheme requirements	-		
	- Easy and direct verification of PD&P protection processes and commitments due to third party certification of themselves	-	-	
	- Increased competition between existing schemes	+		
	- Easier compliance with PD&P protection regulations	NA		
Certified entities or scheme subscribers	- Independently certified compliance, performance and commitments in relation to PD&P protection obligations	+	- Process update costs, certification compliance costs and accreditation costs (Costs of adherence to scheme)	●●
	- Enhanced trust and confidence in products and services by data subjects	+	- Cost of seal (certification and evaluation fees)	●
	- Improved market standing (image/turnover) in relation to customers connected to the certified PD&P processes	NA	- Scheme maintenance costs, including human resource and training costs	●●
	- Competitive and market	+		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	advantage due to better customer perception (reputation) and relationships		-	
	- Improved internal processes measures, awareness of PD&P obligations, and best practices	+		
	- Independent external PD&P assurance/proof	+		
	- Increased burden related to additional processes for PD&P protection	- -		
	- Privacy and data protection disputes redress	+		
	- Regulatory and enforcement burden	- -		
Standardisation and certification bodies	- Widening of institutional tasks of standardisation	+++	- Scheme design costs	● ● ●
			- Cost of coordination	● ● ● ●
	- Need to assess and harmonise potentially conflicting standards and other, analogous, initiatives	- - -	- Cost of maintenance	● ●
			- Monitoring costs	● ● ●
			- Scheme administration costs, human resources and training	● ● ●
	- Requirements of different stakeholders (coordination and harmonisation)	- - -	-	
	- Certification burden optimisation	- -		
	- Protection of PD&P	+		
	- Awareness of PD&P and practices	++		
Industry	- Overall improvement in privacy and data protection	+	-	
	- Encouragement of good practices and demonstration of corporate social responsibility	+		
	- Boost to industry image, reputation and relations with the public, consumers and data subjects	+		
	- Increase in public trust and confidence	+		
Internal Market	- Consolidation of the Internal Market	+		
	- Fostering economic growth	NA		
	- Strengthening of the competitiveness of European companies	NA		
	- Creating critical mass in PD&P regulatory enforcement	NA		
European society	- European Union regulatory harmonisation	+		
	- Better personal data and privacy protection	+		
	- Regulatory and enforcement burden	- - -		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	- Increase in EU standards of privacy and data protection	+		
Regulation and policy making	- Achievement of EU-level policy and regulatory objective	-	- Policy-making and regulatory costs, cost of coordination, including standard set-up	● ●
	- Administrative impact and impact on compliance and enforcement	+	- (Scheme) design costs	● ●
			- Cost of maintenance, cost of administration, cost of scheme operation	● ● ●
	- Capacity to create a harmonised playing field concerning the protection of individual rights and the freedom to act	+	-	
	- Easily see and verify privacy commitments	+		
	- Greater privacy information and awareness	+ +		
	- Implementation and maintenance of data protection measures	+		
	- Level of heterogeneity of approaches and fragmentation	-		
	- Potential for fragmentation	- -		
	- Policy-making impact	+		
	- Quick and accessible privacy and data protection disputes redress	-		
	- Reduction in regulatory and enforcement burden	- -		
	- Relation to existing legislation and interaction with existing mechanisms	+		
	- Strength of regulatory measure	+		
International community	- Creation of a reference for the international support to PD&P protection	- - -	Nil	
	- Improvement of cross-border circulation of privacy sensitive products and services handling personal data	+		
	- Improvement of personal data & privacy protection of EU citizens in their relationships with cross-border partners.	-		

Table 3 Impacts and costs of option 1

6.2 INCORPORATION OF EU DATA PROTECTION REQUIREMENTS INTO AN EXISTING EU CERTIFICATION SCHEME

This option, as shown in section 5.1.2, involves introducing the requirements of the GDPR into one (or more) established certification scheme (such as those in the field of security or other relevant areas). The table below outlines the impacts and costs for this option:

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
Individuals	- Easily and reliably verify PD&P rules respect and commitments	++	- Nil (assuming individuals, data subjects, or relying parties will not have to bear any costs specifically related to the scheme).	
	- Improved trust and confidence	++		
	- Improved PD&P awareness	++		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	++		
	- Support the decision making on products and services in relation to protection of PD&P	++		
	- Easier protection of the data subject, (consumer) rights, provision of means and facilitation of disputes redress	++		
Relying parties or users	- Easily and reliably verify respect of PD&P rules and commitments	++	- Nil (assuming individuals, data subjects, or relying parties will not have to bear any costs specifically related to the scheme).	
	- Improved trust and confidence	++		
	- Improved PD&P awareness	+		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	++		
	- Support the decision making on products and services in relation to the protection of PD&P	+		
	- Easier protection of data subject (consumer) rights, also providing facilitates means of disputes redress	++		
Existing privacy certification schemes	- Adherence to improved PD&P standards and to good practices	+	- Update and integrate certification schemes to comply with the EU seal scheme	● ●
	- Improved accountability and enhanced trust and confidence	++	- Accreditation cost	● ●
	- Improved market standing in relation to seal purchasers related to the certified PD&P processes	++	- Additional costs of scheme maintenance and operation, including regulatory approval costs and human resources and training costs	● ●
	- Additional burden to comply with EU scheme requirements	- -		
	- Easy and direct verification of PD&P protection processes and commitments due to third party certification of themselves	- -	-	
	- Increased competitiveness between existing schemes	- - -		
	- Easier compliance with PD&P protection regulations	+		
Certified entities or scheme subscribers	- Independently certified compliance, performance and commitments in relation to PD&P protection obligations	++	- Process update costs, certification compliance costs and accreditation costs (Costs of adherence to schemes)	● ●
	- Enhanced trust and confidence in products and services by data subjects	+	- Cost of seal (certification and evaluation fees)	●
	- Improved market standing (image/turnover) in relation to customers related to the certified PD&P processes	+	- Scheme maintenance costs, including human resource and training costs	●
	- Competitive and market	+		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	advantage due to better customer perception (reputation) and relationships		-	
	- Improved internal processes measures, awareness of PD&P obligations, and best practices	+		
	- Independent external PD&P assurance/proof	++		
	- Increased burden related to additional processes for PD&P protection	- - -		
	- Privacy and data protection disputes redress	+		
	- Regulatory and enforcement burden	-		
Standardisation and certification bodies	- Widening of institutional tasks of standardisation	+	- Scheme design costs	● ●
			- Cost of coordination	● ● ●
	- Need to assess and harmonise potentially conflicting standards and other, analogous, initiatives	+	- Cost of maintenance	● ●
			- Monitoring costs	● ●
			- Scheme administration costs, human resources and training	● ●
	- Requirements of different stakeholders (coordination and harmonisation)	++	- Loss of some certified entities due to changes in the selected certification scheme	● ●
	- Certification burden optimisation	- -		
	- Protection of PD&P	++		
	- Awareness of PD&P regulations and practices	+++		
Industry	- Overall improvement in privacy and data protection	++		
	- Encouragement of good practices and demonstration of corporate social responsibility	++		
	- Boost to industry image, reputation and relations with the public, consumers and data subjects	++		
	- Increase in public trust and confidence	++		
Internal Market	- Consolidation of the Internal Market	+++		
	- Favouring economic growth	NA		
	- Strengthening of the competitiveness of European companies	+		
	- Creating critical mass in PD&P regulatory enforcement	++		
European society	- European Union regulatory harmonisation	++		
	- Better personal data and privacy protection	+		
	- Regulatory and enforcement burden	- -		
	- Increase in EU standards of privacy and data protection	++		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
Regulation and policy making	- Achievement of EU-level policy and regulatory objective	+	- Policy-making and regulatory costs, cost of coordination, including standard set-up	●
	- Administrative impact and impact on compliance and enforcement	- -	- (Scheme) design costs	●
			- Cost of maintenance, cost of administration, cost of scheme operation	● ●
	- Capacity to create a harmonised playing field concerning the protection of individual rights and the freedom to act	++	-	
	- Easily see and verify privacy commitments	++		
	- Greater privacy information and awareness	+ +		
	- Implementation and maintenance of data protection measures	++		
	- Level of heterogeneity of approaches and fragmentation	+		
	- Uniform regulation	+		
	- Policy-making impact	++		
	- Quick and accessible privacy and data protection disputes redress	NA		
	- Reduction in regulatory and enforcement burden	- -		
	- Relation to existing legislation and interaction with existing mechanisms	++		
	- Strength of regulatory measure	++		
International community	- Creation of a reference for the international support to PD&P protection	+	Nil	
	- Improvement of cross-border circulation of privacy sensitive products and services handling personal data	+		
	- Improvement of personal data & privacy protection of EU citizens in their relationships with cross-border partners.	**NA**		

Table 4 Impacts and costs of option 2

6.3 ACCREDITATION OF CERTIFIERS BY AN EU-LEVEL BODY

As shown in section 5.1.3, this option envisages a specialist EU-level body or organisation (either new or existing) accrediting privacy seal schemes against the criteria set either by the Commission or the EDPB, (or against another agreed EU standard) for privacy seals. The table below outlines the impacts and costs for this option:

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
Individuals	- Easily and reliably verify PD&P rules respect and commitments	+++	- Nil (assuming that individual, data subjects and other relying parties will not have to bear any cost related	
	- Improved trust and confidence	++		
	- Improved PD&P awareness	++		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+++	to the scheme)	
	- Support the decision making on products and services in relation to the protection of PD&P	++		
	- Easier protection of the data subject, (consumer) rights, provision of means and facilitation of disputes redress	+++		
Relying parties or users	- Easily and reliably verify respect of PD&P rules and commitments	+++	- Nil (assuming that individual, data subjects and other relying parties will not have to bear any cost related to the scheme)	
	- Improved trust and confidence	++		
	- Improved PD&P awareness	++		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+++		
	- Support the decision making on products and services in relation to the protection of PD&P	++		
	- Easier protection of data subject (consumer) rights, also providing facilitates means of disputes redress	+++		
Existing privacy certification schemes	- Adherence to improved PD&P standards and to good practices	+++	- Update and integrate certification schemes to comply with the EU seal scheme	●●
	- Improved accountability and enhanced trust and confidence	+++	- Accreditation cost	●●●
	- Improved market standing in relation to seal purchasers related to the certified PD&P processes	+++	- Additional costs of scheme maintenance and operation, including regulatory approval costs and human resources and training costs	●●●
	- Additional burden to comply with EU scheme requirements	- -		
	- Easy and direct verification of PD&P protection processes and commitments due to third party certification of themselves	++	-	
	- Increased competitiveness between existing schemes	- -		
	- Easier compliance with PD&P protection regulations	+++		
Certified entities or scheme subscribers	- Independently certified compliance, performance and commitments in relation to PD&P protection obligations	+++	- Process update costs, certification compliance costs and accreditation costs (Costs of adherence to schemes)	●●
	- Enhanced trust and confidence in products and services by data subjects	++	- Cost of seal (certification and evaluation fees)	●
	- Improved market standing (image/turnover) in relation to customers related to the certified PD&P processes	++	- Scheme maintenance costs, including human resource and training costs	●●
	- Competitive and market advantage due to better customer perception (reputation) and	++		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	relationships			
	- Improved internal processes measures, awareness of PD&P obligations, and best practices	+++		
	- Independent external PD&P assurance/proof	+++		
	- Increased burden related to additional processes for PD&P protection	- -		
	- Redress of privacy and data protection disputes	+++		
	- Regulatory and enforcement burden	-		
Standardisation and certification bodies	- Widening of institutional tasks of standardisation	+	- Scheme design costs	●●●●
			- Cost of coordination	●●●●
	- Need to assess and harmonise potentially conflicting standards and other, analogous, initiatives	+++	- Cost of maintenance	●●●●
			- Monitoring costs	●●●
			- Scheme administration costs, human resources and training	●●●●
	- Requirements of different stakeholders (coordination and harmonisation)	+++	-	
	- Certification burden optimisation	+		
	- Protection of PD&P	+++		
	- Awareness of PD&P regulations and practices	+++		
Industry	- Overall improvement in privacy and data protection	++	- Process update costs - Certification compliance - costs and accreditation costs (Costs of adherence to scheme) - Cost of seal (certification and evaluation fees)	●●
	- Encouragement of good practices and demonstration of corporate social responsibility	++		
	- Boost to industry image, reputation and relations with the public, consumers and data subjects	++		
	- Increase in public trust and confidence	++		
Internal Market	- Consolidation of the Internal Market	+++		
	- Favouring economic growth	+		
	- Strengthening of the competitiveness of European companies	+		
	- Creating critical mass in PD&P regulatory enforcement	+		
European society	- European Union regulatory harmonisation	+++		
	- Better personal data and privacy protection	+(+)		
	- Regulatory and enforcement burden	-		
	- Increase in EU standards of privacy and data protection	+++		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
Regulation and policy making	- Achievement of EU-level policy and regulatory objective	+++	- Policy-making and regulatory costs, cost of coordination, including standard set-up	●●
	- Administrative impact and impact on compliance and enforcement	- -	- (Scheme) design costs	●
			- Cost of maintenance, cost of administration, cost of scheme operation	●
	- Capacity to create a harmonised playing field concerning the protection of individual rights and the freedom to act	+++	-	
	- Easily see and verify privacy commitments	+++		
	- Greater privacy information and awareness	+++		
	- Implementation and maintenance of data protection measures	+++		
	- Level of heterogeneity of approaches and fragmentation	- -		
	- Uniform regulation	+++		
	- Policy-making impact	+++		
	- Quick and accessible privacy and data protection disputes redress	NA		
	- Reduction in regulatory and enforcement burden	- -		
	- Relation to existing legislation and interaction with existing mechanisms	+++		
	- Strength of regulatory measure	+++		
International community	- Creation of a reference for the international support to PD&P protection	+++	Nil	
	- Improvement of cross-border circulation of privacy sensitive products and services handling personal data	++		
	- Improvement of personal data & privacy protection of EU citizens in their relationships with cross-border partners.	+		

Table 5 Impacts and costs of option 3

6.4 CREATION OF A HARMONISED STANDARD FOR EU PRIVACY SEALS

As shown in section 5.1.4, this option envisages the creation of a harmonised European standard or family of standards for privacy certification schemes through the European standardisation (EN) framework. The table below outlines the impacts and costs for this option:

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
Individuals	- Easily and reliably verify PD&P rules respect and commitments	+	- Nil (assuming that individual, data subjects and other relying parties will not	

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	- Improved trust and confidence	+	have to bear any cost related to the seal)	
	- Improved PD&P awareness	+		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	++		
	- Support the decision making on products and services in relation to protection of PD&P	+		
	- Easier protection of the data subject, (consumer) rights, provision of means and facilitation of disputes redress	+		
Relying parties or users	- Easily and reliably verify respect of PD&P rules and commitments	++	- Nil (assuming that individual, data subjects and other relying parties will not have to bear any cost related to the seal)	
	- Improved trust and confidence	+		
	- Improved PD&P awareness	+		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+++		
	- Support the decision making on products and services in relation to the protection of PD&P	++		
	- Easier protection of data subject (consumer) rights, also providing facilitates means of disputes redress	++		
Existing privacy certification schemes	- Adherence to improved PD&P standards and to good practices	++	- Update or integrate certification schemes to comply	● (●)
	- Improved accountability and enhanced trust and confidence	++	- Accreditation cost	●●
	- Improved market standing in relation to seal purchasers related to the certified PD&P processes	+	- Additional costs of scheme maintenance and operation, including regulatory approval costs and human resources and training costs	●●
	- Additional burden to comply with EU scheme requirements	- (-)		
	- Easy and direct verification of PD&P protection processes and commitments due to third party certification of themselves	++	-	
	- Increased competitiveness between existing schemes	++		
	- Easier compliance with PD&P protection regulations	++		
Certified entities or scheme subscribers	- Independently certified compliance, performance and commitments in relation to the PD&P protection obligations	+	- Process update costs, certification compliance costs and accreditation costs (Costs of adherence to schemes)	● (●)
	- Enhanced trust and confidence in products and services by data subjects	+	- Cost of seal (certification and evaluation fees)	●
	- Improved market standing (image/turnover) in relation to	+	- Scheme maintenance costs, including human resource	●●

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	customers related to the certified PD&P processes		and training costs	
	- Competitive and market advantage due to better customer perception (reputation) and relationships	+	-	
	- Improved internal processes measures, awareness of PD&P obligations, and best practices	+++		
	- Independent external PD&P assurance/proof	+		
	- Increased burden related to additional processes for PD&P protection	**+ (-)**		
	- Privacy and data protection disputes redress	**+ (+)**		
	- Regulatory and enforcement burden	**(+) -**		
Standardisation and certification bodies	- Widening of institutional tasks of standardisation	+++	- Scheme design costs	●●●●
			- Cost of coordination	●●
	- Need to assess and harmonise potentially conflicting standards and other, analogous, initiatives	+++	- Cost of maintenance	●●
			- Monitoring costs	●
			- Scheme administration costs, human resources and training	●●
			-	
	- Requirements of different stakeholders (coordination and harmonisation)	+++		
	- Certification burden optimisation	+		
	- Protection of PD&P	+++		
	- Awareness of PD&P regulations and practices	+++		
Industry	- Overall improvement in privacy and data protection	+	- Process update costs - Certification compliance - costs and accreditation costs (Costs of adherence to scheme) - Cost of seal (certification and evaluation fees)	●●
	- Encouragement of good practices and demonstration of corporate social responsibility	++		
	- Boost to industry image, reputation and relations with the public, consumers and data subjects	++		
	- Increase in public trust and confidence	+		
Internal Market	- Consolidation of the Internal Market	+		
	- Favouring economic growth	NA		
	- Strengthening of the competitiveness of European companies	+		
	- Creating critical mass in PD&P regulatory enforcement	NA		
European society	- European Union regulatory harmonisation	+		
	- Better personal data and privacy protection	+		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	- Regulatory and enforcement burden	- -		
	- Increase in EU standards of privacy and data protection	+		
Regulation and policy making	- Achievement of EU-level policy and regulatory objective	+	- Policy-making and regulatory costs, cost of coordination, including standard set-up	●●●●
	- Administrative impact and impact on compliance and enforcement	- -	- Scheme design costs	●
			- Cost of maintenance, cost of administration, cost of scheme operation	**(●)**
	- Capacity to create a harmonised playing field concerning the protection of individual rights and the freedom to act	++	-	
	- Easily see and verify privacy commitments	++		
	- Greater privacy information and awareness	+		
	- Implementation and maintenance of data protection measures	+++		
	- Level of heterogeneity of approaches and fragmentation	+++		
	- Uniform regulation	+++		
	- Policy-making impact	++		
	- Quick and accessible privacy and data protection disputes redress	+		
	- Reduction in regulatory and enforcement burden	- -		
	- Relation to existing legislation and interaction with existing mechanisms	+++		
	- Strength of regulatory measure	**+ (+)**		
International community	- Creation of a reference for the international support to PD&P protection	+++	Nil	
	- Improvement of cross-border circulation of privacy sensitive products and services handling personal data	+		
	- Improvement of personal data & privacy protection of EU citizens in their relationships with cross-border partners.	+		

Table 6 Impacts and costs of option 4

6.5 (EU CRITERIA-BASED) CERTIFICATION BY NATIONAL DATA PROTECTION AUTHORITIES

This option (section 5.1.5) envisages that while the criteria for award of an EU privacy seal would be set centrally (presumably, either by the European Commission or the EDPB, once the GDPR comes into effect, or the Article 29 Data Protection Working Party until such time), the scheme itself would be run by Member State data protection authorities (DPAs). The table below outlines the impacts and costs for this option:

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
Individuals	- Easily and reliably verify PD&P rules respect and commitments	+++	- Nil (assuming that individual, data subjects and other relying parties will not have to bear any cost related to the seal)	
	- Improved trust and confidence	+++		
	- Improved PD&P awareness	+++		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+++		
	- Support the decision making on products and services in relation to the protection of PD&P	++		
	- Easier protection of the data subject, (consumer) rights, provision of means and facilitation of disputes redress	+++		
Relying parties or users	- Easily and reliably verify respect of PD&P rules and commitments	+++	- Nil (assuming that individual, data subjects and other relying parties will not have to bear any cost related to the seal)	
	- Improved trust and confidence	+++		
	- Improved PD&P awareness	+++		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+++		
	- Support the decision making on products and services in relation to protection of PD&P	+++		
	- Easier protection of data subject (consumer) rights, also providing facilitates means of disputes redress	+++		
Existing privacy certification schemes	- Adherence to improved PD&P standards and to good practices	+	- Update and integrate certification schemes to comply with the EU seal scheme	NA
	- Improved accountability and enhanced trust and confidence	0	- Accreditation cost	NA
	- Improved market standing in relation to seal purchasers related to the certified PD&P processes	0	- Additional costs of scheme maintenance and operation, including regulatory approval costs and human resources and training costs	NA
	- Additional burden to comply with EU scheme requirements	0		
	- Easy and direct verification of PD&P protection processes and commitments due to third party certification of themselves	0	-	
	- Increased competitiveness between existing schemes	+		
	- Easier compliance with PD&P protection regulations	+		
Certified entities or scheme subscribers	- Independently certified compliance, performance and commitments in relation to PD&P protection obligations	+++	- Process update costs, certification compliance costs and accreditation costs (Costs of adherence to schemes)	●●
	- Enhanced trust and confidence in products and services by data subjects	+++	- Cost of seal (certification and evaluation fees)	●
	- Improved market standing (image/turnover) in relation to customers related to the certified PD&P processes	++	- Scheme maintenance costs, including human resource and training costs	●●
	- Competitive and market advantage	+++		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	due to better customer perception (reputation) and relationships		-	
	- Improved internal processes measures, awareness of PD&P obligations, and best practices	+++		
	- Independent external PD&P assurance/proof	+++		
	- Increased burden related to additional processes for PD&P protection	-		
	- Privacy and data protection disputes redress	++		
	- Regulatory and enforcement burden	-		
Standardisation and certification bodies	- Widening of institutional tasks of standardisation	NA	- Scheme design costs	●
			- Cost of coordination	●
	- Need to assess and harmonise potentially conflicting standards and other, analogous, initiatives	NA	- Cost of maintenance	●
			- Monitoring costs	●
			- Scheme administration costs, human resources and training	●
	- Requirements of different stakeholders (coordination and harmonisation)	NA	-	
	- Certification burden optimisation	NA		
	- Protection of PD&P	NA		
	- Awareness of PD&P regulations and practices	NA		
Industry	- Overall improvement in privacy and data protection	+++	- Process update costs - Certification compliance - costs and accreditation costs (Costs of adherence to scheme) - Cost of seal (certification and evaluation fees)	●●
	- Encouragement of good practices and demonstration of corporate social responsibility	+++		
	- Boost to industry image, reputation and relations with the public, consumers and data subjects	+++		
	- Increase in public trust and confidence	+++		
Internal Market	- Consolidation of the Internal Market	+++		
	- Favouring economic growth	NA		
	- Strengthening of the competitiveness of European companies	NA		
	- Creating critical mass in PD&P regulatory enforcement	+		
European society	- European Union regulatory harmonisation	+++		
	- Better personal data and privacy protection, increase in standards	+++		
	- Regulatory and enforcement burden	- -		
Regulation and policy making	- Achievement of EU-level policy and regulatory objective	+++	- Policy-making and regulatory costs, cost of coordination, including standard set-up	●●●●
	- Administrative impact and impact on compliance and enforcement	- -	- Scheme design costs	●●●

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
			- Cost of maintenance, cost of administration, cost of scheme operation	●●●
	- Capacity to create a harmonised playing field concerning the protection of individual rights and the freedom to act	+++	-	
	- Easily see and verify privacy commitments	+++		
	- Greater privacy information and awareness	+++		
	- Implementation and maintenance of data protection measures	+++		
	- Level of heterogeneity of approaches and fragmentation	+++		
	- Uniform regulation	+++		
	- Policy-making impact	+++		
	- Quick and accessible privacy and data protection disputes redress	+(++)		
	- Reduction in regulatory and enforcement burden	- -		
	- Relation to existing legislation and interaction with existing mechanisms	+++		
	- Strength of regulatory measure	++(+)		
International community	- Creation of a reference for the international support to PD&P protection	+++	Nil	
	- Improvement of cross-border circulation of privacy sensitive products and services handling personal data	+++		
	- Improvement of personal data & privacy protection of EU citizens in their relationships with cross-border partners.	+++		

Table 7 Impacts and costs of option 5

6.6 FULL REGULATION (FURTHER EXTENSION OF ARTICLE 39)

This policy option envisages a full regulatory approach to EU privacy seals, as outlined in section 5.1.6. The table below outlines the impacts and costs for this option:

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
Individuals	- Easily and reliably verify PD&P rules respect and commitments	+++	- Nil (assuming that individual, data subjects and other relying parties will not have to bear any cost related to the scheme)	
	- Improved trust and confidence	+++		
	- Improved PD&P awareness	+++		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+++		
	- Support the decision making on products and services in relation to the protection of PD&P	+++		
	- Easier protection of the data subject, (consumer) rights,	+++		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	provision of means and facilitation of disputes redress			
Relying parties or users	- Easily and reliably verify respect of PD&P rules and commitments	+++	- Nil (assuming that individual, data subjects and other relying parties will not have to bear any cost related to the scheme)	
	- Improved trust and confidence	+++		
	- Improved PD&P awareness	+++		
	- Support the verification of PD&P protection measures and the fulfilment of relevant obligations	+++		
	- Support the decision making on products and services in relation to the protection of PD&P	+++		
	- Easier protection of data subject (consumer) rights, also providing facilitates means of disputes redress	+++		
Existing privacy certification scheme	- Adherence to improved PD&P standards and to good practices	+++	- Update and integrate certification schemes to comply with the EU seal scheme	● ● ●
	- Improved accountability and enhanced trust and confidence	+++	- Accreditation cost (cost of being certified)	NA
	- Improved market standing in relation to seal purchasers related to the certified PD&P processes	+++	- Additional costs of scheme maintenance and operation, including regulatory approval costs and human resources and training costs	NA
	- Additional burden to comply with EU scheme requirements	NA		
	- Easy and direct verification of PD&P protection processes and commitments due to third party certification of themselves	NA	-	
	- Increased competitiveness between existing schemes	+++		
	- Easier compliance with PD&P protection regulations	+++		
Certified entities or scheme subscribers	- Independently certified compliance, performance and commitments in relation to PD&P protection obligations	+++	- Process update costs, certification compliance costs and accreditation costs (Costs of adherence to schemes)	● ●
	- Enhanced trust and confidence in products and services by data subjects	+++	- Cost of seal (certification and evaluation fees)	● ●
	- Improved market standing (image/turnover) in relation to customers related to the certified PD&P processes	++	- Scheme maintenance costs, including human resource and training costs	● ●
	- Competitive and market advantage due to better customer perception (reputation) and relationships	++	-	
	- Improved internal processes measures, awareness of PD&P obligations, and best practices	+++		
	- Independent external PD&P assurance/proof	+++		
	- Increased burden related to additional processes for PD&P protection	- -		
	- Privacy and data protection	+		

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	disputes redress			
	- Regulatory and enforcement burden	-		
Standardisation and certification bodies	- Widening of institutional tasks of standardisation	NA	- Scheme design costs	●
			- Cost of coordination	●
	- Need to assess and harmonise potentially conflicting standards and other, analogous, initiatives	+++	- Cost of maintenance	●
			- Monitoring costs	●
			- Scheme administration costs, human resources and training	●
	- Requirements of different stakeholders (coordination and harmonisation)	NA	-	
	- Certification burden optimisation	++		
	- Protection of PD&P	+++		
	- Awareness of PD&P regulations and practices	+++		
Industry	- Overall improvement in privacy and data protection	+++		
	- Encouragement of good practices and demonstration of corporate social responsibility	**++(+)**		
	- Boost to industry image, reputation and relations with the public, consumers and data subjects	**++(+)**		
	- Increase in public trust and confidence	+++		
Internal Market	- Consolidation of the Internal Market	+++		
	- Favouring economic growth	NA		
	- Strengthening of the competitiveness of European companies	NA		
	- Creating critical mass in PD&P regulatory enforcement	NA		
European society	- European Union regulatory harmonisation	+++		
	- Better personal data and privacy protection	+++		
	- Regulatory and enforcement burden	- -		
	- Increase in EU standards of privacy and data protection	+++		
Regulation and policy making	- Achievement of EU-level policy and regulatory objective	+	- Policy-making and regulatory costs, cost of coordination, including standard set-up	● ● ● ●
	- Administrative impact and impact on compliance and enforcement	- -	- Scheme design costs	● ● ● ●
			- Cost of maintenance, cost of administration, cost of scheme operation	● ● ● ●
	- Capacity to create a harmonised playing field concerning the protection of individual rights and the freedom to act	+++	-	

Stakeholder experiencing impact	Qualification of impact	Scale of impact	Associated costs (description)	Scale of costs
	- Easily see and verify privacy commitments	+++		
	- Greater privacy information and awareness	+++		
	- Implementation and maintenance of data protection measures	+++		
	- Level of heterogeneity of approaches and fragmentation	+++		
	- Uniform regulation	+++		
	- Policy-making impact	++		
	- Quick and accessible privacy and data protection disputes redress	+++		
	- Reduction in regulatory and enforcement burden	- - -		
	- Relation to existing legislation and interaction with existing mechanisms	+++		
	- Strength of regulatory measure	+++		
International community	- Creation of a reference for the international support to PD&P protection	+++	Nil	
	- Improvement of cross-border circulation of privacy sensitive products and services handling personal data	+++		
	- Improvement of personal data & privacy protection of EU citizens in their relationships with cross-border partners.	+++		

Table 8 Impacts and costs of option 6

The above assessment indicates the potential impacts and costs of the six options, shaped following an ex-ante impact assessment approach. This assessment was developed based on a set of harmonised impact areas, examined in relation to the key stakeholders identified as relevant to the six options. The assessment was based on a collaborative, expert assessment by the study team, using the levels described in the introduction to this section, drawing on the research findings, insights into the different options and a multiple review of the different impacts and cost evaluations.

As outlined in the introduction to this section, this assessment faced a number of challenges. First, the research and analysis of existing privacy seals could not produce any generalisable, quantitative information on costs specifically costs of operating the schemes; even fee pricing structures are not disclosed. Second, the cost of setting up a privacy seal scheme, for any of the six options – which frequently are not mutually exclusive – is strongly dependent on the specific adoption and implementation choices. Third, the different practical choices of implementing the different policy options may involve additional different bodies besides the key organisation(s) outlined in the option, depending on the final form of the certification scheme and its core objectives. Fourth, each proposed option has a smaller or larger set of implementation sub-options or may take different forms depending on the policy and resource-based decisions about the objectives of the EU scheme, the certification criteria and requirements, the certification process, the delegation of certification activities to third party organisations, the disputes and redress mechanisms, etc. Based on this, any policy sub-options may also have different impacts and different costs.

Some strong proportionalities or inverse proportionalities are clearly recognisable: for example, the higher the regulatory harmonisation sought across the EU, the higher the policy making costs. We would like to emphasise that the impacts are relative to specific stakeholder groups.

Based on the positive and negative impact ratings and of the associated costs, we can summarise the six options as follows:[69]

Option	Positive impact	Negative impact	Level of cost
(1) Encouraging and supporting the GDPR certification regime			
Individuals	7	0	0
Relying parties or users	6	0	0
Existing privacy certification schemes	3	2	6
Certified entities or scheme subscribers	6	4	5
Standardisation and certification bodies	6	8	15
Industry	4	0	0
Internal market	1	0	0
European society	3	3	0
Regulation and policy making	9	7	7
International community	1	4	0
TOTALS	**46**	**28**	**33**

Table 9 Summary – impact and costs of option 1

Option	Positive impact	Negative impact	Level of cost
(2) Incorporation of EU data protection requirements into an existing EU certification scheme			
Individuals	12	0	0
Relying parties or users	10	0	0
Existing privacy certification schemes	6	7	6
Certified entities or scheme subscribers	9	4	4
Standardisation and certification bodies	9	2	13
Industry	8	0	0
Internal market	6	0	0
European society	5	2	0
Regulation and policy making	17	4	4
International community	2	0	0
TOTALS	**84**	**19**	**27**

Table 10 Summary – impact and costs of option 2

Option	Positive impact	Negative impact	Level of cost
(3) Accreditation of certifiers by an EU-level body			
Individuals	15	0	0
Relying parties or users	15	0	0

[69] Please note that in several cases the impacts or costs are not assessable (NA), which biases the summaries.

Existing privacy certification schemes	14	4	8
Certified entities or scheme subscribers	18	3	5
Standardisation and certification bodies	14	0	19
Industry	8	0	2
Internal market	6	0	0
European society	8	1	0
Regulation and policy making	27	6	4
International community	6	0	0
TOTALS	**131**	**14**	**38**

Table 11 Summary – impact and costs of option 3

Option	Positive impact	Negative impact	Level of cost
(4) Creation of a harmonised standard for EU privacy seals			
Individuals	7	0	0
Relying parties or users	11	0	0
Existing privacy certification schemes	11	2	6
Certified entities or scheme subscribers	12	2	5
Standardisation and certification bodies	16	0	11
Industry	6	0	2
Internal market	2	0	0
European society	3	2	0
Regulation and policy making	22	4	6
International community	5	0	0
TOTALS	**95**	**10**	**30**

Table 12 Summary – impact and costs of option 4

Option	Positive impact	Negative impact	Level of cost
(5) (EU criteria-based) certification by national data protection authorities			
Individuals	17	0	0
Relying parties or users	18	0	0
Existing privacy certification schemes	3	0	0
Certified entities or scheme subscribers	19	2	5
Standardisation and certification bodies	0	0	5
Industry	12	0	2
Internal market	4	0	0
European society	6	2	0
Regulation and policy making	33	4	10
International community	9	0	0
TOTALS	**121**	**8**	**22**

Table 13 Summary – impact and costs of option 5

Option	Positive impact	Negative impact	Level of cost
(6) Full regulation (further extension of Article 39)			
Individuals	18	0	0

Relying parties or users	18	0	0
Existing privacy certification schemes	15	0	3
Certified entities or scheme subscribers	17	3	6
Standardisation and certification bodies	8	0	5
Industry	12	0	0
Internal market	3	0	0
European society	9	2	0
Regulation and policy making	30	5	12
International community	9	0	0
TOTALS	**139**	**10**	**26**

Table 14 Summary – impact and costs of option 6

The following table and diagram show the net impact of the options (positive minus negative impacts identified before in the individual tables) and the potential cost levels.

Options	Option #	Net impact	Cost levels
Full regulation (further extension of Article 39)	6	129	26
Accreditation of certifiers by an EU-level body	3	117	38
(EU criteria-based) certification by national data protection authorities	5	113	22
Creation of a harmonised standard for EU privacy seals	4	85	30
Incorporation of EU data protection requirements into an existing EU certification scheme	2	65	27
Encouraging and supporting the GDPR certification regime	1	18	33

Table 15 Summary – net impact and costs of options

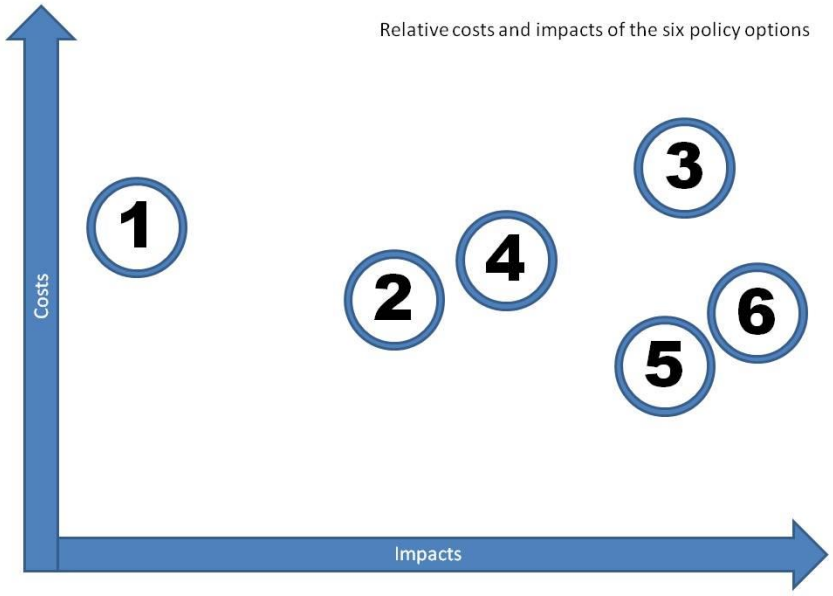

Figure 1 Relative costs and impacts of the six policy options

According to the table and figure, the option with the most impact (comparatively), seems to be the full regulatory option (option 6), closely followed by the option on accreditation of certifiers by an EU-level body (option 3) and (EU criteria-based) certification by national data

protection authorities (option 5). The options that score low on net impact are the options on incorporation of EU data protection requirements into an existing EU certification scheme (option 2), and encouraging and supporting the GDPR certification regime through soft measures (option 1). Creation of a harmonised standard for EU privacy seals (option 4) fits somewhere in the middle. That said, the options that produce the most impacts are also the ones that would take the longest to implement, and that build on the strictest assumptions (for collated estimate of timeframes for each option, see Table 2). In particular, options 4, 5 and 6 would require at least 5 years to implement, from the time the Regulation is adopted. However, it might be possible to implement options 1, 2 and 4 (or combinations of these or the other options) in parallel to the adoption of the GDPR (to the extent that they do not conflict with the spirit and any requirements of the GDPR).

As to the costs, the option that scores the highest on collated cost is the option envisaging accreditation of certifiers by an EU-level body (option 3), while the EU (criteria-based) certification by national data protection authorities (option 5) and full regulation options score low on costs.

Option:	1) Encourage GDPR regime	2) Incorporate into existing scheme	3) Accreditation of certifiers by an EU-level body	4) Creation of a harmonised standard for EU privacy seals	5) (EU criteria-based) certification by national data protection authorities	6) Full regulation
Individuals	7/0	12/0	15/0	7/0	17/0	18/0
Relying parties	6/0	10/0	15/0	11/0	18/0	18/0
Existing certification schemes	3/2	6/7	14/4	11/2	3/0	15/0
Certified entities	6/4	9/4	18/3	12/2	3/0	15/0
Standardisation bodies	6/8	9/2	14/0	16/0	0/0	8/0
Industry	4/10	8/0	8/0	6/0	12/0	12/0
Internal market	1/0	6/0	6/0	2/0	4/0	3/0
European society	3/3	5/2	8/1	3/2	6/2	9/2
Regulatory and policy making	9/7	17/4	27/6	22/4	33/4	30/5
International community	1/4	2/0	6/0	5/0	9/0	9/0
	High positive impact					
	High negative impact					

Table 16 Cumulative impacts on stakeholders

The above table plots the cumulative impact (positive/negative) of each policy option against the different categories of stakeholders. The information is derived from the previous tables, but demonstrates more clearly which options have the largest impact upon different types of

stakeholders. The cells of the table shaded in blue show the policy option with the highest positive impact for each stakeholder group, and the cells shaded in orange show the policy option with the highest negative impact for each stakeholder group. Many stakeholders will be strongly impacted by policy options 3, 5 and 6. This method of analysis demonstrates that none of the analysed policy options is, by itself, likely to have a significant negative impact on individuals and relying parties (other than that represented by costs, including indirectly through taxation). The issue then becomes one of identifying the option(s) that create the greatest positive impact. The use of soft measures to support GDPR certification regime appears particularly problematic in this analysis as it contains the highest potential negative impacts for many stakeholders.

7 REFLECTIONS ON THE CRITERIA AND REQUIREMENTS FOR AN EU PRIVACY SEAL

The GDPR does not specifically prescribe the criteria and requirements for an EU privacy seal scheme; however it is important to consider the criteria at this stage, given their importance and centrality to the success of any adopted certification scheme. The criteria and requirements of a privacy seal scheme form the underlying basis of the scheme. It is what helps build confidence and trust in the scheme. A privacy seal scheme is only as strong or as weak as its criteria.

This section provides some reflections on the criteria for an EU privacy seal scheme based on the findings of the Study and the current state of play. First, it reiterates the findings of the Study on criteria, then examines what the General Data Protection Regulation (GDPR) states about criteria, outlines some core elements for the criteria framework for an EU privacy seal, and finally identifies some challenges, barriers and possible next steps.

7.1 STUDY FINDINGS ON THE CRITERIA OF THE ANALYSED EXISTING PRIVACY SEAL SCHEMES

The research into, and analysis of the 25 privacy and related schemes in Task 1 shows that these schemes are heterogeneous in nature; all underpinned by different types of criteria and requirements.[70] Some of these criteria are based on law – EU (EuroPriSe), national (CNIL label is based on French data protection law) or international or a combination of these (for example, the ePrivacyseal criteria is based on EU, German law, and the IAB Online Behavioural Advertising (OBA) Framework). The criteria of some schemes are derived from industry standards and good practices or a combination of these. For example, the MRS Fair Data criteria are based on the Fair Data principles, Code of Conduct, UK Data Protection Act 1998, ISO standards, the Safe Harbor Framework, the Data Seal initiative, MRS Data Protection Guidance Document. Some schemes often have a code of conduct or best practice criteria that build upon data protection and privacy law, but may also 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 (e.g. ESRB, WebTrust, TÜViT Trusted Site Privacy, TRUSTe).

[70] Rodrigues et al, *Inventory*, op. cit., 2013.

We reiterate the key findings (specifically, the concerns) of the Study on the criteria underlying existing privacy seal schemes. These are important and should be taken into account in the development of criteria for an EU-wide privacy seal scheme.

Pick and mix

Existing privacy seal schemes, operating in a largely self-regulatory environment, are free to determine their own criteria and requirements. As stated before, these might be based only on law, and sometimes a blend of law, industry standards and good practice. This has several consequences: the criteria and requirements of some schemes may be rigorous and robust, while the criteria of other schemes is often weaker and may enable applicants to get certified on the basis of meeting requirements that give the impression of good data protection and privacy, when it might not be the case.

Vague and abstract

The criteria of many of the analysed schemes are often shrouded in vague and abstract terms. Some schemes provide no detailed information on privacy and data protection or measures to enhance these. 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 achieved are left ambiguous. In general, many existing privacy seal schemes lack robust and transparent criteria with clear standards and workable enforcement. The vast majority of schemes have ambiguous, abstract or vague criteria, and make abstract promises about what is being protected, or what guarantees are being made to the end user. We do find however, that within the EU, seals aligned with data protection law have more specific, open, and therefore robust criteria.

Not particularly supportive of data subject rights

The wording of the criteria and requirements of some schemes is sometimes tailored to meet scheme applicants' need to 'demonstrate' some form of privacy reassurance in a minimalist fashion; this means that the rights of data subjects get compromised or are not adequately accounted for. Many schemes focus more upon information security than specific data subject rights despite claiming to enhance and protect these. Some schemes only provide broad assurances unsupported or substantiated by detailed requirements. Many schemes are not in line with controller and processor obligations under data protection law (for instance, 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 must 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.

Lack of clarity about their scope

Often the certification criteria of the existing schemes are very generic; some examples of copy-paste efforts with no forethought given to the end objective, what lies within the scope of certification and what does not (i.e. what do the criteria and requirements apply to and what is excluded from its scope). Schemes often also fail to specify from where they derive their privacy and data protection criteria (i.e. law, industry standards, or codes of conduct). Further, they often fail to clarify whether the criteria are national or international in scope.

Lack of information about the development, review and continued relevance of the criteria to sector

Few of the analysed privacy seal schemes provide adequate information on the process of how the criteria were developed. For greater transparency, it is necessary, as determined in relation to the established EU sectoral certification schemes analysed in Task 2, that the criteria development is a public, multi-stakeholder process. Many privacy seal schemes often fail to provide information on whether the criteria are stagnant or reviewed on an ongoing basis (and if so, how often and what actions are taken as a result of the review). They also do not specify (apart from a few) that if criteria are amended, whether certified entities need to be re-evaluated. Information is also lacking on how the criteria meet the need to be continually relevant to the varied sectors they are targeted at, given that technological developments are a constant challenge to the sectors privacy seals operate in.

Not public or easily accessible

While a majority of certification schemes (such as EuroPriSe, TRUSTe, Trusted Shops, WebTrust, etc.) do publicise and present their criteria, there are other certification schemes that do not publish the criteria or requirements used for the award of seals on their main website. For 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."[71] 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).

Not robust enough

While many of the privacy seal schemes express impressive objectives (such as building confidence and trust), their criteria and requirements do not seem robust enough to help achieve those objectives. Confidence (and trust) are related to particular measures such as data protection, security or guaranteed transactions, but are frequently left abstract in the criteria (perhaps deliberately to ensure flexibility, but the concern remains that this might allow organisations a way out of meeting stricter requirements). Further, the requirements or criteria of many of the analysed schemes, with very few exceptions, are not tested against the general EU data protection law especially the requirements for proportionality and necessity of personal data processing. While another expressed objective of schemes is to help resolve

[71] Transaction Guard, Privacy Policy Verified Seal. http://www.transactionguard.com

disputes, often scheme requirements fail to mandate on their subscribers the requirement for a good dispute resolution process, often only insisting upon the bare minimum.

7.2 STUDY CONCLUSIONS ON WHAT IS NEEDED FOR MORE EFFECTIVE CRITERIA

Based on the above findings, we can draw certain conclusions in relation to the criteria and requirements of an EU-wide privacy seal scheme. These conclusions are based on the research of Tasks 1, 2, and 3 of the Study and the feedback from the Task 5 workshop.

First, we need a **collaborative and consultative approach** to developing criteria and requirements. This is supported by the Parliament's position on Article 39. This is also evident from Task 2 – a collaborative and consultative approach to criteria makes for a more broad-based ownership of the criteria and inclusionary effect of the scheme.[72] The options analysis in section 5 also supports the need for this approach.

Second, the development of criteria and requirements for an EU privacy seal scheme must be **transparent.** It is important to ensure the process of criteria development is visible, open and enables stakeholders to contribute, as required. It would also ensure greater receptiveness, and possibly, wider validation and acceptance of the criteria.
Third, the criteria must be **relevant to technological developments and public expectations**. Not only should the scheme demonstrate publicly (and transparently) the relevant criteria for evaluating applicants, it must also demonstrate that such criteria are instrumental and effective in achieving the level of data protection and privacy prescribed by EU law, while being relevant to technological developments and societal expectations. The criteria should take into account or be able to accommodate both contextual and cultural sensitivities.

Fourth, the criteria should **support data protection and privacy compliance** and not enable certified organisations to dodge their responsibilities or adopt other dubious practices.

Fifth, the criteria should be **freely and easily accessible**. Publishing a scheme's criteria and requirements not only serves the business purposes of the scheme (applicants can discern the compliance requirements for applying and acquiring a seal), it also serves public awareness purposes (i.e., the public or relying parties can examine the requirements or criteria a seal represents and make an informed decision about whether to trust a seal or not).

Sixth, the criteria must be **clear, specific** and **coherent** in nature and scope. The criteria should also have a **sound basis**, be **robust** and **dynamic.** The purposes of the criteria should be clearly defined, along with the scope.

Seventh, the criteria should be **reviewed** (and if necessary revised) at least every three to five years.[73] The scheme should outline measures for **regular review, improvements and innovations** to the scheme. To this end, the scheme's operator should hold consultations with relevant stakeholders to take their views into account.

[72] Rodrigues et al, *Task 2*, op. cit., 2013.
[73] Ecolabel criteria are evaluated every three-five years. This allows the criteria to reflect technical innovation, such as evolution of materials or production processes, and emission reductions and changes in the market. Ecological criteria are reviewed prior to their expiration and may be revised. The board contributes to the revision of the criteria, but the Commission is responsible for their final drafting.

Finally and more crucially, the criteria should be drafted in such a manner that enables them to be **rigorously applied and promotes a harmonised implementation** across the EU.

7.3 THE GDPR ON CRITERIA

The Commission's draft of the GDPR (2012), Article 39 (2) states:

> 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.[74]

The Parliament's amendment to Article 39 (2) reads:

> The Commission shall be empowered to adopt, **after requesting an opinion of the European Data Protection Board and consulting with stakeholders, in particular industry and non-governmental organisations**, 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 **paragraphs 1a to 1h, including requirements for accreditation of auditors**, conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries. **Those delegated acts shall confer enforceable rights on data subjects.**[75]

Thus, Parliament supports a collaborative approach to the specification of criteria and requirements.

The underlying objectives that should guide the criteria development (i.e. the objectives of the certification mechanisms) can be found in Recital 77 of the GDPR. Recital 77 (Parliament version) states:

> In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and standardised marks should be encouraged, allowing data subjects to quickly, reliably and verifiably assess the level of data protection of relevant products and services. [76]

Thus, we see that the main role of certification mechanisms, data protection seals and standardised marks would be to enhance transparency and compliance with this Regulation – the criteria and requirements for an EU privacy seal scheme must take this into account.

7.4 CORE ELEMENTS OF CRITERIA DISTILLED FROM GDPR

[74] 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

[75] European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), A7-0402/2013, 21 Nov 2013.

[76] European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), A7-0402/2013, 21 Nov 2013.

Based on a review of the GDPR provisions and the supporting guidance, the following provisions of the GDPR (briefly presented) will be relevant for incorporation in the criteria of the EU privacy seal scheme:

1. **Principles relating to personal data processing (**Article 5)
    - Fair, lawful, transparent processing of personal data
    - Data collection for specified, explicit and legitimate purposes
    - Adequate, relevant and limited data collection (data minimisation)
    - Data accuracy
    - Time and purpose restricted data retention (storage minimisation)
    - Effectiveness
    - Integrity
    - Accountability (data processing under responsibility, liability of the controller)
2. **Lawfulness of processing** (Article 6)
3. **Conditions for consent** (Article 7)
4. **Processing of personal data of a child** (Article 8)
    - Processing of personal data of a child below 13 only lawful if and to extent consent is given or authorised by the child's parent or legal guardian
    - Controller to make reasonable efforts to verify such consent.
5. **Prohibition on processing of special categories of personal data (except as permitted)** (Article 9)
6. **General principles for data subject rights:** clear and unambiguous rights for the data subject which shall be respected by the data controller, provision of clear and easily understandable information regarding processing of personal data (Article 10a)
7. **Information to data subject (controller obligation)** (Article 14)
8. **Data subject rights**
    - The right of access (Article 15), rectification (Article 16) and erasure of their data (Article 17)
    - The right to obtain data (Article 15)
    - The right to object (Articles 19, 20)
    - The right to lodge a complaint with the competent data protection authority and to bring legal proceedings (Articles 73-75)
    - The right to compensation and damages resulting from an unlawful processing operation (Article 77)
9. **Data protection by design and by default** (Article 23)
    - Implementation of appropriate and proportionate technical and organisational measures and procedures
    - Entire lifecycle management of personal data from collection to processing to deletion
    - Systematic focus on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data.
10. **Documentation requirements for controllers and processors** (Article 28)
11. **Security of processing** (Article 30)
    - Implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing
    - Security policy requirements:
        - The ability to ensure that the integrity of the personal data is validated

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data
- The ability to restore the availability, access to data in a timely manner in the event of a physical or technical incident
- Additional security measures for sensitive personal data
- A process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans

12. **Notification of a personal data breach to the supervisory authority** (Article 31)
13. **Communication of breach to data subject** (Article 32)
14. **Data protection impact assessment** (Article 33)
15. **Compliance with the requirements for prior authorisation/prior consultation of the supervisory authority** (Article 34 (1) and (2))
16. **Designation of a data protection officer** (Article 35)
17. **Audit/external oversight mechanisms to ensure the verification of the effectiveness of controller/processor obligations** (Article 22).

7.5 OTHER REQUIREMENTS AND CONDITIONS

We also recognise that there are other criteria, requirements and conditions for an EU privacy seal that are not covered by the GDPR. These must be taken into account and embedded as part of the EU privacy seal requirements. These include:

1. **Correct and proper definition of the use of seal and certification**: Use of the certification and seal (and any qualifying text) must only be permitted as authorised. The conditions for using the certification and seal, other than as is prescribed, must also be determined and clearly specified. For instance, should the seal be only used for illustrative purposes or could it also be used for marketing purposes? Who is authorised to use the seal, where and how it can be used, must also be prescribed. Unauthorised use of the seal should be strictly prohibited and appropriate penalties specified.

2. **Cooperation with certification body**: This should mandate that all participants cooperate with the certification body in any respect that is necessary for the acquiring, the continued enjoyment of the certification, or for re-certification purposes. For example, providing information when requested in a timely manner, permitting access to auditors for inspections and evaluations.

3. **Notification of material changes**: Certified entities must notify the certification body of any material changes that have been made to the certified technology, process, practice or system. This should be done prior to making the change so that the certification body can advise the certified entity of any measures it needs to take in relation to its certification obligations The certified entity might also be required to notify affected individuals (and the public) of the change.

4. **Re-certification:** This might be relevant to maintain certification and verify compliance at the end of the validity period (or in some cases on an annual basis). There should be a clear list of criteria and specification of the conditions for re-certification. Recertifying would help an organisation prove that its data protection and privacy practices continue to meet the criteria of the EU privacy seal.

5. **Requirements for recognition within the Union and in third countries**: this would potentially include having a valid EU privacy seal, a valid listing on the register.

6. **Withdrawal, revocation of certification**: Many seal schemes do not provide information on the reasons and method for the revocation of their seal. This makes 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. Grounds for withdrawal, revocation of certification should include: breach or violation of scheme requirements, violation of EU data protection or privacy law, abuse of the certification/seal, failure to allow access for audits and inspection and failure to address concerns raised by data protection authorities. The implications of withdrawal or revocation of certifications must be clearly set out.

While these criteria, generally relate to certification, in relation to option 3 (accreditation of certifiers), we can envisage also, the following criteria and requirements for accrediting privacy certification schemes: clearly defined scope, target of evaluation and certification policies and procedures; well defined standards and requirements; transparency and accountability; an efficient evaluation and certification process, audits, complaints and redress process.

7.6 CHALLENGES AND BARRIERS TO CRITERIA

Some of the challenges and barriers to criteria that an EU privacy seal scheme should take into account include:

1. **Overly prescriptive criteria**: Overly prescriptive criteria in an EU privacy seal might make it more rigid and inflexible and may cause efficiency failures. The criteria might not be able to take into account differences in technologies and data processing sectors.
2. **Criteria and requirements that stifle innovation**: this will not be well received by the industry and it will adversely affect their interests in particular and harm the public interest, in general.
3. **Creation of unnecessary, additional obligations and excessive compliance burdens**: If the criteria create unnecessary, additional obligations and excessive compliance burdens, this might affect the overall cause of the scheme (though in a certain sense, it might promote a higher level of privacy and data protection).

7.7 POTENTIAL FUTURE STEPS

The potential steps for setting out the criteria for the EU privacy seal could include:

1. Preparation of a draft criteria framework.
2. Informal consultation with stakeholders.
3. Revision of the criteria framework based on the consultation.
4. Formal consultation with select stakeholders.
5. EDPB/Article 29 WP Opinion on the criteria.
6. Adoption of the criteria.

8 CONCLUSION

This report attempts to demonstrate how best to encourage the development of an EU-wide privacy seals scheme by examining six key possible options or scenarios that support the GDPR to this effect, identifying their challenges, assessing their impacts and costs and providing some guidance and recommendations on how to implement these options.

While there are a number of policy options possible, in this report we specifically examined six policy options that best fit the vision envisaged in the GDPR: Encouraging and supporting the GDPR certification regime (option 1), incorporation of EU data protection requirements into an existing EU certification scheme (option 2), accreditation of certifiers by an EU level body (option 3), creation of a harmonised standard for EU privacy seals (option 4), (EU criteria-based) certification by national data protection authorities (option 5) and full regulation (option 6). As outlined before, each of the options has its pros and cons, and carries with it its own resource implications. However, there is no longer an option to "do nothing"- this has no value given legislative developments, and the rising need to enhance personal data protection through robust, yet accessible measures. Doing nothing would only reinforce the status quo.
Based on the analysis and the priorities outlined in Task 3[77] and the exercise conducted in section 6 of this report, option 6 (full regulation), option 3 (accreditation of certifiers by an EU-level body) and option 5 (EU criteria-based) certification by national data protection authorities) seem worthy for further exploration as potential courses of action, either by themselves or in combination with elements outlined in the other options.[78] These three options appear to have the potential for the most positive impact on individuals. However, we recognise that the relevance and potential of any chosen option will depend on the end goal or objective sought to be accomplished, the available resources, and whether that option (either alone or in combination with others) is best suited to achieve that objective.

We recommend the following irrespective of which option is chosen and the form it is finally implemented (either singly or in combination):

- Whatever the option(s) chosen and scheme(s) adopted, it should be rigorously and consistently applied and promote a harmonised data protection and privacy standard across the EU.
- The objectives, and the scope of the scheme should be precise and clear to all stakeholders.
- While the options might provide the tools to support, simplify and facilitate data protection and privacy compliance, they should not in any way limit the rights of the data subjects or enable certified organisations to dodge their responsibilities or adopt other dubious practices.
- It might be useful to encourage and/or facilitate the use of multiple options if this has the effect of strengthening fundamental rights to personal data protection and privacy.

With regard to the criteria and requirements for an EU privacy seal scheme, we specifically reiterate that:

[77] De Hert et al, *Task 3*, op. cit., 2014.
[78] We recognise that the full regulation option might be too prescriptive and might not accord well with the exponential pace of technology development and data processing operations.

- The development of criteria should be an inclusive, open and transparent process.
- The criteria should take into account differences in technologies and data processing sectors and be relevant to them, and to public expectations.
- The criteria and requirements should not stifle innovation or create unnecessary, additional obligations and excessive compliance burdens.
- The criteria should be drafted in such a manner as to support data protection and privacy compliance and not enable certified organisations to dodge their responsibilities or adopt other dubious practices.
- The criteria should be freely and easily accessible to the public and to potential certified entities.
- The criteria must be robust, dynamic, clear, specific, coherent (in nature and scope) with a sound basis. Criteria should be reviewed (and if necessary revised) at least every three to five years.
- The criteria should be drafted in such a manner that enables them to be rigorously applied and promotes a harmonised standard across the EU.

9 REFERENCES

1. BSI, "How Standards Help Consumers". http://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/how-standards-help-consumers/
2. Cargill, Carl F., "Why Standardisation Efforts Fail", *Journal of Electronic Publishing*, Vol. 14, Issue 1, Summer 2011. http://quod.lib.umich.edu/j/jep/3336451.0014.103?rgn=main;view=fulltext
3. CEN, "CEN Compass: The world of European Standards". http://www.din.de/sixcms_upload/media/2896/CEN_compass.pdf
4. Cini, Michael, "The soft law approach: Commission rule-making in the EU's state aid regime", *Journal of European Public Policy*, Vol. 8, No. 2, 2001, pp. 192 - 207.
5. Cram, Laura, "The European Commission as a multi-organization: social policy and IT policy in the EU", *Journal of European Public Policy*, Vol.1, No. 2, 1994, pp. 195-217
6. Data Guidance, "UK: ICO to launch privacy seals scheme 'within the year'", *Privacy This Week*, 27 March 2014.http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2258.
7. De Hert, Paul, Vagelis Papakonstantinou, Rowena Rodrigues, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki, *Task 3 Challenges and Possible Scope of an EU Privacy Seal Scheme, D3.3, Final report*, Study on EU Privacy Seals, European Commission Joint Research Centre, Institute for Protection and Security of the Citizen, January 2014.
8. European Commission, "Country-specific recommendations 2013: frequently asked questions" 29 May 2013. http://europa.eu/rapid/press-release_MEMO-13-458_en.htm
9. European Commission, "Learning from each other to improve R & I policies". http://ec.europa.eu/research/era/partnership/coordination/method_of_coordination_en.htm
10. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe COM(2012) 529 final, Brussels, 27 September 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
11. European Commission, Enterprise and Industry, Directorate-general, New Approach Industries, Tourism and CSR Standardisation, *Vademecum on European Standardisation*, Part II, European standardisation in support of European policies, Chapter 4.1, Role and preparation of mandates, 15 October 2009. http://ec.europa.eu/enterprise/policies/european-standards/files/standards_policy/vademecum/doc/preparation_of_mandates_web_en.pdf
12. 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.
13. European co-operation for Accreditation (EA). http://www.european-accreditation.org
14. European Parliament and the Council, Directive 2002/58/EC 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 July 2002, pp. 37–47.
15. European Parliament and the Council, Directive 2006/24/EC 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, 13 April 2006, pp. 54–63.
16. European Parliament and the Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *OJ L* 281, 23 Nov 1995, pp. 0031-0050.
17. European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), A7-0402/2013, 21 Nov 2013. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
18. ISO, *ISO/IEC 17021:2011 Conformity assessment -- Requirements for bodies providing audit and certification of management systems*, Stage: 90.93, 17 January 2013.http://www.iso.org/iso/catalogue_detail?csnumber=56676
19. Jacobsson, K., "Beyond deliberation and discipline: soft governance in the EU employment policy" in Ulrika Morth (ed.), *Soft Law in Governance and Regulation: An Interdisciplinary Analysis*, Edward Elgar Publishing, 2004.
20. Nesbitt, Brian (ed.), *Pumping Manual International, Handbook of Pumps and Pumping*, Elsevier, Oxford, 2005, p. 266
21. Poullet, Y., J-M. Van Gyseghem, J-P. Moiny, J. Gerard, & C. Gayrel, "Data Protection in the Clouds", in Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Springer 2011, pp. 377-409.
22. Rodrigues, Rowena, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki, Paul De Hert & Vagelis Papakonstantinou, *Task 2: Comparison with other EU certification schemes, D2.4, Final report*, Study on EU Privacy Seals, European Commission Joint Research Centre, Institute for Protection and Security of the Citizen, November 2013.
23. Rodrigues, Rowena, David Barnard-Wills, David Wright, Paul De Hert and Vagelis Papakonstantinou, *Inventory and Analysis of Privacy Certification Schemes: Final Report Study Deliverable 1.4,* Publications Office of the European Union, Luxembourg, 2013. http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26190/?CatalogCategoryID=CXoKABst5TsAAAEjepEY4e5L
24. Rodrigues, Rowena, David Wright and Kush Wadhwa, "Developing a privacy seal scheme (that works)", *International Data Privacy Law*, Vol. 3, Issue 2, first published online 1 February 2013. doi:10.1093/idpl/ips037
25. Sabel, Charles F., and Jonathan Zeitlin, "Learning from Difference: The New Architecture of Experimentalist Governance in the EU", *European Law Journal*, Vol. 14, No. 14, May 2008, pp. 271-327.
26. The European Parliament and the Council, 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, *OJ L* 218, 13 August 2008, pp. 30-47.
27. Trubek, David M., and Louise G. Trubek, "Hard and Soft Law in the Construction of Social Europe: the Role of the Open Method of Coordination", *European Law Journal*, Vol. 11, No. 3, May 2005, pp. 343-364.
28. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), "EuroPriSe 2.0 – Continuation of the European Privacy Seal (EuroPriSe) by

EuroPriSe GmbH – Extended range of certifications", 14 November 2013. https://www.european-privacy-seal.eu/ws/EPS-en/Press-releases
29. Van Hoboken, Joris, "The EU out of Focus: Some Deeper Truths about the European Approach to Privacy Law and Policy, 31 March 2014. http://ssrn.com/abstract=2418636
30. Weber, Franziska, "European Integration assessed in the light of the 'Rules vs. Standards debate'", *European Journal of Law and Economics*, Vol. 35, 2013, pp. 187-210.
31. Zeitlin, Jonathan, "Is the OMC an Alternative to the Community Method?", in Renaud Debousse (ed.), *The Community Method: Obstinate or Obsolete*? Palgrave MacMillan, Basingstoke, 2009.

European Commission
EUR 26834 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: **EU Privacy seals project**

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

Luxembourg: Publications Office of the European Union

2014 – 93 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-40330-9

doi:10.2788/14722

LB-NA-26834-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2788/14722

ISBN 978-92-79-40330-9

Publications Office