12 April 2017

Discussion Paper

Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms

Centre for Information Policy Leadership GDPR Implementation Project
April 2017

CIPL's TOP TEN MESSAGES ON GDPR CERTIFICATIONS

1. Certification should be available for a product, system, service, particular process or an entire privacy program.

2. There is a preference for a common EU GDPR baseline certification for all contexts and sectors, which can be differentiated in its application by different certification bodies during the certification process.

3. The Commission and/or the EDPB, in collaboration with certification bodies and industry, should develop the minimum elements of this common EU GDPR baseline certification, which may be used directly, or to which specific other sectoral or national GDPR certifications should be mapped.

4. The differentiated application of this common EU certification to specific sectors may be informed by sector-specific codes of conduct.

5. Overlap and proliferation of certifications should be avoided so as to not create consumer/stakeholder confusion or make it less attractive for organisations seeking certification.

6. Certifications must be adaptable to different contexts, scalable to the size of company and nature of the processing, and affordable.

7. GDPR certifications must be consistent with and take into account other certification schemes with which they need to be able to interact and/or be as much interoperable as possible, such as ISO/IEC Standards, EU-US Privacy Shield, APEC CBPR and the Japan Privacy Mark.

8. Developing a common EU-wide GDPR certification for purposes of data transfers pursuant to Article 46(2)(f) should be a priority for the Commission and/or the EDPB.

9. Organisations should be able to leverage their BCR approvals to receive or streamline certification under an EU GDPR certification.

10. DPAs should incentivise and publicly affirm certifications as a recognised means to demonstrate GDPR compliance, and a mitigation in case of enforcement, subject to the possibility of review of specific instances of non-compliance.

1. INTRODUCTION

1.1 Certifications, seals and marks under the GDPR as promising instruments for data protection

Certifications, seals and marks have the potential to play a significant role in enabling companies to achieve and demonstrate organisational accountability and, more specifically, GDPR compliance for some or all of their services, products or activities. The capability of certifications to provide a comprehensive GDPR compliance structure will be particularly useful for SMEs. For large and multinational companies, certifications may, in addition, facilitate business arrangements with business partners and service providers.

However, certifications must not be made mandatory, but should be treated only as one of many optional tools for companies. There must be no inference of non-compliance if a company chooses not to obtain certification.

In addition, certifications, seals and marks can be used as accountable, safe and efficient cross-border data transfer mechanisms under the GDPR, provided they are coupled with binding and enforceable commitments, including with regard to data subject rights. Finally, there is potential for creating interoperability with other legal regimes, as well as with similar certifications, seals and marks in other regions or in other policy domains.

These instruments present real benefits for all stakeholders, including DPAs and, most importantly, individuals. They have the potential to assist organisations in delivering better compliance and more effective protection for individuals given that certified organisations will have made a conscious effort to become GDPR compliant and will have been reviewed by a third party in that respect.

This is why CIPL generally supports the certifications, seals and marks in the GDPR. However, it is crucial that certifications are effectively operated, incentivised and clearly accompanied by benefits for certified organisations. Otherwise, organisations will be reluctant to invest time and money in obtaining and maintaining GDPR certifications on top of the many other certifications and requirements to which they are already subject.

1.2 The CIPL GDPR Project

This paper is produced by the Centre for Information Policy Leadership at Hunton & Williams (CIPL) as part of its project (CIPL GDPR Project) on the consistent interpretation and implementation of the GDPR.

The CIPL GDPR Project—a multiyear-long project launched in March 2016—aims to establish a forum for dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the member states and academics on the consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and comments.

CIPL aims to provide input to the Article 29 Working Party (WP29) on a number of priority areas, identified in CIPL's GDPR Project work plans for 2016 and 2017.[1] This is the fourth white paper in this series, following earlier CIPL papers on DPO, Risk, and OSS and Lead Authority.[2]

1.3 CIPL's Certifications Paper

In this paper, CIPL aims to provide the WP29, the EU Commission and data privacy practitioners with input on certifications, seals and marks under the GDPR and the roles of these instruments as accountability tools and cross-border data transfer mechanisms.

The paper intends to facilitate the development of certifications, seals and marks under the GDPR[3] in a way that is pragmatic and benefits all stakeholders.[4]

CIPL notes that there are both similarities and differences between certifications and approved codes of conduct under the GDPR. Although the synergies between both tools must be identified, CIPL will address codes of conduct separately, at a later stage.

2. BENEFITS OF CERTIFICATIONS

Adherence to approved certification mechanisms under Article 42 GDPR may be used as an element in demonstrating compliance with the GDPR obligations of the controller and processor. Moreover, certification mechanisms have the potential to significantly contribute to effective and efficient privacy protection for individuals in a globalised world. They should evolve into real bridges between different legal regimes and accountability frameworks.

Specifically, CIPL has identified the following benefits of certifications to key stakeholders—individuals, organisations, DPAs and the overall digital ecosystem:

2.1 Benefits for individuals

Certifications carry tangible benefits for individuals.

- **Create trust.** Certifications have the potential of increasing individuals' trust and confidence in a certified organisation's handling of their personal data. This in turn may result in individuals'

[1] See https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_work_plan_17_march_2017.pdf

[2] See https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf; https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_the_gdpr_one-stop-shop_30_november_2016.pdf; https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

[3] See Appendixes I and II for a summary of the GDPR certification provisions.

[4] In this paper, we will use the term "certifications" to encompass seals and marks (without foreclosing a discussion about whether there can be differences between these three concepts).

wanting to engage more with a certified organisation and participating in the digital economy more freely.

- **Greater transparency.** Certification ensures better transparency of processing practices of the organisation, making it easier for individuals to understand and assess relevant data practices and their merits.

- **Effective privacy protection.** Individuals may regard certification as a demonstration of commitment to and compliance with effective and rigorous data protection and complaint resolution practices. Adherence to certification mechanisms by organisations ultimately may deliver better compliance and outcomes for individuals, with their data's being more effectively protected.

2.2 Benefits for Certified Organisations

If implemented effectively, certifications may convey a number of key benefits to organisations.

- **Demonstrate accountability and compliance.** Certification is an element of demonstrating GDPR compliance and accountability.[5] This is an internal benefit vis-à-vis management, the board and shareholders. It also benefits an organisation externally in its relationships with DPAs, individuals, clients and business partners. It builds confidence and trust in the organisation with these external stakeholders, as well as with the wider public.

- **Operationalising compliance.** Certifications translate high-level GDPR requirements into operational compliance steps that are closely tailored by subject-matter experts to the organisation and their privacy management programs. This may result in more relevant, fit-for-purpose and effective privacy and data management programs.

- **Scalable for SMEs and start-ups.** For SMEs and start-ups, well-conceived and properly implemented certifications can serve as scalable and at the same time comprehensive compliance mechanisms that make relevant GDPR accountability obligations less burdensome, less costly and easier to implement, in particular for organisations that do not yet have fully developed privacy management programs or their own internal privacy experts and staff. The third-party certification body will have the expertise and the obligation to ensure that the certifying organisation has policies and processes in place that comply with the GDPR. This improves both organisational compliance and privacy protections for individuals.

- **B2B due diligence and risk management.** In B2B relationships, certification may efficiently demonstrate GDPR compliance and accountability on the part of the processor or service provider. For the same reason, it may also serve as an effective risk-management tool in B2B relationships by lowering the risk profile of the certified processors or providers, thereby directly lowering the risk level of the involved processing as well as the need for DPIAs and/or prior consultations with DPAs.

[5] Article 24(3) GDPR.

- **Enabling cross-border data transfers.** Certification provides legal certainty to organisations by enabling them to share personal data lawfully outside the EU and across borders, provided that certification is coupled with binding and enforceable commitments.

- **Interoperable and global reach.** The effect of a GDPR certification as a cross-border transfer mechanism could be even stronger when the certification is made interoperable with other, similar mechanisms, thereby extending the certification's geographic coverage and reach. Examples of systems with which GDPR certification could be made interoperable include the ISO Cloud Privacy and Security Standard, the Japan Privacy Mark and the APEC Cross-Border Privacy Rules (CBPR).

- **Mitigating factor in DPA oversight and enforcement**. In addition to serving as demonstration of compliance in the context of audits or other inquiries by DPAs, certification is potentially a mitigating factor in connection with GDPR enforcement and the determination of sanctions.

2.3 Benefits for DPAs

Certification mechanisms have the potential for supporting the oversight missions of DPAs and making it possible for them to leverage their scarce resources more effectively.

- **Reduce oversight workload.** Where certification bodies take on and share the burdens of supervision and oversight with the DPAs, this has the potential of reducing the DPAs' workload.

- **Compliance.** Certifications may result in improved outcomes and more effective compliance on the ground due to the certification process, therefore reducing the enforcement burdens of DPAs.

- **Reduce complaint handling.** Because certifications may include complaint handling and dispute resolution mechanisms, they can help reduce DPAs' involvement in resolving individual complaints. This aspect of certifications will be important in practice, given that the GDPR gives DPAs a significant complaint-handling role.

- **Transparency.** Certification will require organisations to disclose their data practices in a transparent and organised fashion vis-à-vis the certification bodies and ultimately DPAs. This will make it easier for DPAs to properly assess these practices as well as possible violations of the GDPR. This, in turn, may drive down the costs and burdens of enforcement actions, both for DPAs and organisations.

2.4 Benefits for the Ecosystem and for Business Partners

The entire business ecosystem, including non-certified businesses, may benefit from certifications.

Because certifications signal a certain level of data protection and the presumption of GDPR compliance, certifications could streamline and shorten B2B due diligence and risk assessment processes between certified and non-certified organisations seeking qualified and trusted business partners in the digital ecosystem. This could lead to a greater speed of doing business and avoid protracted negotiations about privacy and security, benefiting business beyond just certified companies.

3. KEY POINTS AND RECOMMENDATIONS

3.1 GDPR Certification as an Opportunity

Certifications have significant potential as accountability and compliance mechanisms and for delivering privacy protection to individuals. For this potential to be realised, the following conditions must be fulfilled:

- **Promote benefits and incentivise businesses to adopt certifications.** Industry must be given the right incentives to take up certification instruments. This requires putting in place a certification process that is efficient and appropriately fast, scalable and affordable for all sizes of organisations. It also may include promoting the benefits of certifications by allowing certified organisations to transfer data outside the EU or to engage in broader data uses consistent with the GDPR and by recognising them as mitigation in enforcement and other interactions with DPAs. Otherwise, organisations will be reluctant to invest time and money in obtaining and maintaining certifications (in addition to the many other certifications to which they are already subject).

- **Certification granted to a company must also be stable and valid for at least three years** to avoid a constant cycle of re-certification at short intervals. The renewal of GDPR certifications after three years should be as easy and efficient as possible.

- **Emphasise features of building trust and a competitive advantage.** Certifications must be helpful and recognisable to individuals. Individuals must have trust in certifications and be able to rely on them in deciding with whom to do business, thereby providing certified companies or processes a competitive advantage vis-à-vis non-certified companies. In addition, certifications must be capable of engendering trust in the B2B context and provide a competitive advantage in that context as well.

- **Avoid one-size-fits-all.** Certifications should be adaptable, scalable to all sizes of companies and the nature of processing, and affordable without deviating from the core elements of the EU-wide GDPR baseline certification (discussed below at 3.3). This includes controllers and processors, large companies as well as SMEs, start-ups, etc. The adaptability and scalability would go to "how" these core elements are applied in the particular context and which elements may or may not be applicable at all.

- **Allow a variety of certifications.** The GDPR does not specify the object of certification, other than "processing operations" (Art. 42(1)) and "products and services" (Recital 100). In CIPL's view, consistent with the relevant GDPR provisions, the object of a certification can be a product, system or service, a particular process, or an entire privacy program[6] and information management infrastructure, or the full range of an organisation's products and services.[7] Limiting availability of certifications to only products, services or a technical process rather than an entire privacy program would seriously undermine the relevance, usefulness and thus

[6] Any certification of a privacy management program should be based on, or take into consideration as certification referentials, WP 155 BCR for controllers and WP 195 BCR for processors.

[7] Although the certification of DPOs has merits and may support the role of DPOs, we take the view that this specific certification falls outside the scope of Article 42 GDPR.

attractiveness of certifications. In any event, what is to be certified must be clearly articulated and distinguishable from non-certified products, processes, services or programs by and within an organisation. Consumer confusion must be avoided. Finally, not all products or services have to be certified at the same time, but different certifications within one organisation might be staggered.

- **Keep certifications technologically neutral.** Certifications should not be linked to any particular technologies, tools or frameworks that are prone to change over time. However, certifications should be technology-aware, in the sense that they take account of the impact of various technologies on personal data protection.

- **Certifications should reflect or be able to accommodate the latest developments.** Certifications should reflect or be able to accommodate up-to-date standards, current expertise and the most recent techniques. To accomplish this, certifications must be flexible enough to allow their application in contexts where technology and business practices evolve.

- **Benefit from existing certifications, including BCR and avoid bureaucratic and slow processes.** Because certification will normally require real effort and investment of resources from companies, it is important to find ways for organisations to benefit from existing certifications that are GDPR compliant, including Binding Corporate Rules (BCR). Companies will not want to start a process of "re-certification" at additional costs, if they have already been certified on the same or similar standards or requirements, but under a different name, or in different legal regimes or in different jurisdictions. Compliance with existing frameworks should be considered and recognised under the GDPR certification scheme. In short, certifications under the GDPR should not lead to another layer of bureaucracy. (See also discussion of BCR in 3.6 below.)

- **Learn lessons from the BCR approval process**. Lessons that need to be learned include, for example, the slow uptake by companies that may be associated with lengthy and costly processes.

3.2 Relationship between certifications, seals and marks

The GDPR does not specify a difference or relationship between certifications, seals and marks.[8] Indeed, the three concepts are not typically seen as something different but as co-equivalents.

CIPL believes that future work on GDPR certifications, seals or marks should not introduce unwarranted and unnecessary differentiation between these terms. However, it should be explored whether different elements of the certification process can be separated and performed by different actors. Possibly, certain actors could deliver parts of, or intermediate steps towards, a certification, seal or mark that is ultimately issued by a certification body or a DPA.

3.3 The need for one EU baseline certification

To ensure effectiveness and take-up of certifications, CIPL recommends the following:

[8] Certifications, seals and marks are not equal to icons, a transparency tool provided for in Article 12 GDPR. However, they may have a logo, mark or symbol that signifies them, just like an icon may signify a certain privacy or information management and use practice.

- **Preference for one EU baseline certification for all contexts and sectors, with possible differentiation in its application.** Ideally, there would be one baseline EU-wide certification standard—the "common certification" or "European Data Protection Seal" under Article 43(5) of the GDPR—developed under the lead of the Commission or the EDPB in collaboration with certification bodies and industry.

    - This standard or common certification should contain a comprehensive set of certification criteria that are both sufficiently granular and comprehensive to provide for EU-wide consistency and sufficiently high-level and flexible to allow for sector-, industry- and context-specific adaptation and application by certification bodies.

    - This standard or common certification may subsequently be applied taking account of the specific nature and complexity of the specific certifying company, product, service, process or whatever the object of certification might be. Not all the requirements necessarily come into play with each process or organisation. A less complex process or a smaller company may trigger the application of a more limited number of elements of this baseline certification. For example, a processor's certification might focus primarily on the data security elements and omit aspects of the certification not relevant to it.

    - As to differentiation in applying this baseline EU-wide certification between industry sectors, specialised certification bodies (or sophisticated, non-specialised certification bodies that have expertise with multiple or all industries) could specify this baseline certification to the needs, practices and circumstances of a particular industry sector. Approved sector-specific codes of conduct could be one mechanism to facilitate the sectoral-application of a baseline certification standard.

    - CIPL believes that creating separate sectoral or national certifications without reference to a general baseline EU-wide certification may be confusing, inefficient and unnecessary. Existence of a general comprehensive certification standard would enable specialised application and adaption of that baseline to specific sectors, such as pharma, advertising, credit referencing, etc.

    - The GDPR does allow national and EU-wide certifications to work in parallel. However, certifications that currently exist in the EU at the national level (or may exist in the future) should be aligned with this common EU-wide GDPR certification, including GDPR certifications that may already be under development in member states.

    - It is paramount to avoid an overlap and proliferation of certifications and seals in the EU (or elsewhere) as this could lead to confusion for all stakeholders, including individuals, and disencourage organisations from seeking certification altogether.

    - National certifications should be used only for organisations whose privacy programs, services and products are limited to a single member state. These national certifications should not only be issued in full compliance with Art 42(5), but before they are issued, it should also be ensured that they are consistent with each other and the general EU certification. Otherwise, there will be confusion for individuals and businesses moving and operating across the EU.

- There should be a mechanism for companies that are certified at the member states level to have that certification recognised in additional member states and also at the EU level. The Commission is encouraged to use its powers under Art 43(8) and (9) to set up such a mechanism. The EDPB can also set up mutual recognition process for national certifications.

3.4 Certification and compliance

- **Certification as an element of compliance and presumption of compliance** GDPR certification does not necessarily demonstrate full compliance with the GDPR, but it is one of the elements of demonstrating compliance and accountability. However, this one element[9] of compliance should be understood as a strong presumption that a certified product, process or an organisation's privacy program is in compliance. Thus, DPAs should publicly affirm and support the notion that certifications will be treated as a recognised and accepted means for demonstrating compliance. This is, of course, without prejudice to the DPAs' power to take action and enforcement against a certified organisation where there is a cause to do so and to review specific instances of possible non-compliance. It is essential for the success of certification that DPAs fully implement, recognise and honour the compliance function of certifications.

- **Certification could also go beyond compliance.** Certification is primarily an instrument for demonstrating GDPR compliance and should not exceed the requirements set forth in the GDPR. However, certification can also be used to show proactive and enhanced accountability above and beyond compliance. For example, consistent with the certification requirements, certified organisations may provide additional choices for individuals where possible and useful.

- **Certification should be a mitigating factor in the contexts of accountability and enforcement.** CIPL emphasises the importance of GDPR certification in the context of compliance and accountability, with focus on the issue of certification as a mitigating factor. DPAs should use the existence of certification as a mitigating factor in enforcement and when determining fines. DPAs should explicitly confirm this impact of certification to ensure better take-up in the marketplace.

- **Certification should be an aggravating factor only in exceptional cases**. If a certified organisation deliberately or with gross negligence chooses to ignore its certification commitments whilst gaining financial benefit from such certification, the certification may serve as an aggravating factor in an enforcement matter, or in establishing a fine.

- **Absence of certification should have no negative effect.** DPAs must make it clear that the absence of a certification should not result in a negative inference with respect to compliance. Having no certification should not be interpreted to mean that an organisation is less likely to be compliant. However, we acknowledge that there may be peer pressure in cases where one organisation in a sector gets certified for its product, service or compliance program. The rest of the market may follow for that reason alone. In addition, individuals may take note of who is certified and who is not.

[9] Art 24(3) GDPR.

- **Failure in receiving certification should have no negative effect.** Another issue relates to an organisation which applies for but fails to obtain a certification from the certification body or DPA. CIPL believes that being unsuccessful in receiving a certification from a certification body or generally withdrawing from the certification application process should not be reportable to a DPA, nor should it otherwise carry negative inferences with respect to compliance. However, it should be clear that this does not mean that an organisation that failed to certify with one certification body or DPA can then seek certification from another based on the same facts and program. Forum shopping must be avoided.

3.5 GDPR certification in relation to other relevant compliance instruments and frameworks

It is important to clarify the relationship between certification and specific accountability instruments and frameworks. Where possible, existing compliance tools should be integrated in the certification process.

- **Certifications must be consistent and take into account other instruments and frameworks, both within and outside EU**. Certifications based on ISO/IEC Standards, the EU-US Privacy Shield, the APEC CBPR and the Japan Privacy Mark are examples of other systems and frameworks having particular importance in this context. We must avoid unnecessary proliferation of different certification schemes or standards and we should use the GDPR process for creating certifications to harmonise, consolidate and make interoperable existing mechanisms, where possible. This requires an assessment of other data protection certifications already existing in the marketplace, in the EU and globally. Ultimately, companies will favour global schemes that are universally recognised.

- **GDPR certifications should have a streamlining effect**. Certifications should be used to streamline risk assessments, due diligence and contracting processes in B2B relationships (including controller/processors relationships). It should be recognised that GDPR certifications could be a considered in the context of risk assessments required by the GDPR, whereby a certified company, product or service would have a lower risk profile due to the certification.

- **GDPR certifications should not reinvent the wheel.** The functioning of GDPR certifications should be informed by lessons learned from other third-party privacy and security certification systems, such as the APEC CBPR and those based on ISO/IEC standards.

- **Codes of conduct are different instruments, but have similarities to certifications.** Codes of conduct are approved by the DPAs or provided general validity by the EU Commission. Also, they may include an ability to demonstrate adherence to the code similar to certifications. It should be elaborated how the two instruments relate to each other. It should also be considered how approved sector-specific codes of conduct can leverage certifications to support accountability and GDPR compliance in different sectors.

3.6 Certification and other instruments for data transfer, in particular BCR

CIPL notes that there are significant synergies between GDPR certification and BCR, a key instrument for data transfer which received additional recognition in Article 47 GDPR.

- **BCR are a de facto form of certification.** The two instruments are presented as separate concepts, but, arguably, BCR are a de facto form of certification and it makes sense to elaborate the similarities between the two concepts. BCR-approved companies and their executive leadership all regard their BCR as a de facto certification of their privacy compliance program and a "badge of recognition" by DPAs.

- **Recognise the assessments made in the BCR context.** BCR should be considered a specific type of certification. Thus, it should be explicitly recognised that BCR-approved companies may be given credit for their BCR towards GDPR certification in so far as their BCR meet the relevant certification criteria. (See also bullet on BCR in 3.1 above.)

- **Avoid additional re-certification costs.** The coexistence of the BCR and certifications in the GDPR should not lead to additional costs or investment of resources and efforts. That is why companies that have one of the two, should be able to leverage them for obtaining the other at no unnecessary additional cost.

- **Where a GDPR certification is deemed to provide adequate protection for international transfers, assess the relationship between that certification and other transfer mechanisms.** This assessment should in particular include the relationship with other data transfer mechanisms that work on the basis of a similar certification with which the EU schemes need to interact. This includes the EU/US Privacy Shield and the APEC CBPR.

- **Where a GDPR certification is deemed to provide adequate protection for international transfers, create interoperability with other transfer mechanisms**. CIPL recommends maximising the potential for GDPR certifications as cross-border transfer mechanisms. Thus, at a minimum, the development of a baseline certification standard should be recognised as a data transfer instrument, similar to the benefit offered by the BCR. Further, any new transfer-related certifications should, where possible, avoid creating conflicting requirements with other systems. In that connection, CIPL welcomes the Commission's interest in "explor[ing] [ways] to promote convergence between BCR under EU law and the Cross Border Privacy Rules developed by the Asia Pacific Economic Cooperation (APEC) as regards both the applicable standards and the application process under each system."[10] Of course, the same applies to "convergence" efforts between any new EU-based certification or codes and the APEC CBPR. We emphasise that many global companies have a single privacy management program, with all of its essential elements and substantive privacy requirements, that they apply consistently and comprehensively to their processing activities in all countries where they operate. They then leverage this same program to obtain Privacy Shield certification in the US, CBPR in APEC and BCR in Europe, under the respective approval and certification rules.

4. The roles of the various actors and recommendations

The GDPR provides roles to various actors in respect of certification. For instance, the Commission, DPAs and the EDPB all have roles in developing and drafting the standards or criteria for certification, but it is not evident who takes the lead. Also, the GDPR requires the member states, the DPAs, the EDPB and the

[10] Communication from the Commission to the European Parliament and the Council; Exchanging and Protecting Personal Data in a Globalised World, Brussels 10.1.2017, COM (2017) 7 final (emphasis added), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=41157

Commission to encourage the establishment of certification mechanisms. Here, it may be less crucial to lay down who takes the lead, but it would nevertheless be productive if these actors coordinate their efforts and develop a common approach. Regardless of who takes the formal lead, it is crucial that certification bodies and industry stakeholders participate in the development of the certification standards, criteria and mechanisms.

4.1 Member states

- Under the GDPR, (the governments of) member states must "encourage" certifications (Art 42(1)) and must ensure that certification bodies are properly accredited by a DPA or a national accreditation body. They should fulfil these roles under the GDPR in a proactive and consistent manner.

- It is key that member states encourage the certification and accreditation tasks in a coordinated manner, to ensure consistent approaches and avoid discrepancies between the implementation of these mechanisms in the member states.

- The member states' contributions to the delegated acts and the implementing acts (Art 43(8) and (9)) should be assessed in this perspective.

- At the national level, member states should encourage cooperation between DPAs and organisations in non-data protection domains that have experience in certification. Such cooperation should improve the quality and effectiveness of the GDPR certification processes.

4.2 DPAs

- **DPAs** have wide powers under the GDPR. Inter alia, they have the power to issue, renew and revoke certifications, or, where certifications are issued by certification bodies, the DPAs approve the accreditation criteria for such bodies. They also play a key role in the accreditation of certification bodies, which already exist in many member states.

- DPAs also have the power to disapprove or revoke individual certifications provided by certification bodies "where necessary". It should be further elaborated how this power will be implemented in a sensible way without introducing a new layer of review in each case. WP29 guidance should develop the appropriate criteria and a process for when and how to exercise this power, based on the notion that this power should be exercised only in exceptional cases.

- Equally, methods must be developed for DPA review of a third party's certification process, ex ante and/or ex post.

- The accreditation of certification bodies would be a new task for DPAs and does not necessarily fit within their past experiences. It also bears the risk of regulatory capture when the DPAs are required to take enforcement actions against companies, processes, products or services certified by a certification body which the DPA itself has accredited. The risk of regulatory capture is even more pronounced when the DPA itself issues certifications which it must later enforce.

- Thus, CIPL supports a co-regulatory approach with respect to certification, whereby certifications would primarily be provided by third-party certification bodies. (This approach would also help alleviate potential resource issues within the DPAs and potential bottlenecks in the certification process.

4.3 The EDPB (and WP29)

- The EDPB should agree with the Commission on who is in the best position to initiate an EU baseline certification.

- As mentioned, CIPL believes that, to ensure consistency, there should be one baseline EU-wide GDPR certification that would then be applied by different certification bodies (or DPAs) in different contexts. This baseline certification could be developed by or under the leadership of the EDPB or the Commission**.** Both the EDPB and the Commission are in the best position to encourage and ensure an EU-wide harmonised approach on certification.

- Before the EDPB will be effectively established, there is a role to play for the WP29. The WP29 should provide guidance at this stage, mainly on the issues addressed in the various parts of this paper. We encourage the WP29 to provide opportunities for the industry to give input before final issuing of guidance. In addition, the WP29 could start leading a process to develop a baseline GDPR certification, with input by relevant stakeholders, including industry.

- As concerns guidance, CIPL expresses a preference for the WP29's providing guidance at this timely stage over guidance by individual DPAs. This guidance should also encompass further defining the role of the lead DPA in EU-wide certifications.

4.4 The Commission

- The Commission should agree with the EDPB on who is in the best position to initiate an EU baseline certification.

- The GDPR gives the Commission a role to pass further implementing and delegating acts.[11] CIPL believes these provisions include the authority to develop a baseline EU-wide GDPR certification, and we recommend that either the Commission or the WP29 promptly commence that work, which includes seeking input from stakeholders.

- We recommend that the Commission clarify ambiguous elements of Art 43(8) and (9). More specifically, the Commission should clarify the meaning of (1) "specifying the requirements to be taken into account for the certification mechanisms"; (2) technical standards for certification mechanisms and data protection seals and marks"; and (3) "mechanisms to promote and recognise those certification mechanisms, seals and marks". The Commission should also explain how it seeks to put these provisions into effect.

[11] The Commission may adopt delegated acts for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms. (Arts 92 and 43(8) It may also adopt implementing acts to lay down technical standards for certification mechanisms and data protection seals and marks as well as mechanisms to promote and recognise such mechanisms, seals and marks. (Art 43(8))

- We believe the Commission's role under the GDPR includes ensuring the consistent implementation of certifications and seals in the EU, regardless of whether the Commission or EDPB takes the lead in drafting a baseline GDPR certification.

4.5 Certification bodies

- In general, for efficiency and scalability reasons, CIPL expresses a preference for third-party certification by certification bodies over certification by DPAs (see Art 42(5) GDPR). Certification by certification bodies avoids and alleviates potential resource issues and bottlenecks in the DPAs that could result from widespread use of certifications. It protects the DPAs' functional independence.

- Certification by certification bodies should be set up in a way that ensures an effective and practical participation of the private sector in the certification process. Further work is needed on defining how certification bodies and companies seeking certification will assign the risk between themselves that is associated with a potential DPA disapproval of a certification, such as losing the fee spent on the certification process. It should be established how the risks are divided under those circumstances.

4.6 National accreditation bodies

- National accreditation bodies have the task to accredit certification bodies (the same task is attributed to DPAs). To the extent accreditation is performed by national accreditation bodies as opposed to DPAs, such bodies must ensure that their accreditations of GDPR certification bodies are performed by staff with expertise in data protection and other related matters. This must ensure effective application of the GDPR accreditation criteria.

- The yet-to-be developed accreditation criteria that elaborate on the relevant GDPR requirements in Article 43(2) should be open to public comment and industry input before finalisation by the DPAs and/or the EDPB.

4.7 Private sector organisations

- Private sector organisations, including businesses that might seek certification and potential certification bodies, should have a meaningful role in the drafting and development of GDPR certification schemes and criteria. They are in the best position to advise on the potential impacts and practical implementation challenges that may be associated with specific certification criteria and standards.

- This means there should be a regular consultation with industry by member states, DPAs, the WP29/EDPB, the Commission and non-private sector certification and accreditation bodies, following structured consultation procedures. It also means that private sector organisations should have a proactive approach, taking up signals received in the market.

Appendix I -- Summary of GDPR Certification Provisions

I. Certification in the framework of Article 42 GDPR

Member states, DPAs, the EDPB and the EU Commission must encourage establishment of certifications: (Art 42(1),(3)); see also (57(1)(n); (70)(1)(n)).

- At national and particularly at EU level
- For use by controllers and processors
- Voluntary and available through a transparent process

Controllers and processors may use certifications: (Art 42(1),(2); see also (46(2)(f)); (Articles 24(3) and 28(5))

- As an element to demonstrate compliance with the Regulation
- As an element to demonstrate compliance with the obligations of the controller
- Demonstrate sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation (processor)
- Demonstrate appropriate safeguards in third countries for data transfers; certifications must be coupled with enforceable commitments by the controllers or processors in the third country to apply such safeguards

Certification does not reduce GDPR compliance obligations or prejudice the tasks and powers of the DPAs: (42(4))

- But it is one factor that DPAs must take into account in determining administrative fines—it can be both mitigating and aggravating (83(2)(j)(k))

Certifications are issued by certification bodies or the DPA: (42(5); see also 57(1)(o); 58(1)(c) and (2)(h); 58(3)(f))

- On the basis of criteria approved by the DPA (national) or the EDPB (EU DP seal)
- Last up to three years and are renewable (42(7))
- Can be withdrawn by certification bodies or DPAs, if the certification requirements are not or no longer met
- EDPB maintains a publicly available register of all certifications, seals and marks (42(8)); see also 43(6); 70(1)(o))

To obtain certification from a certification body or DPA, organisations must: (42(6))

- Provide all relevant information about the processing activities they seek to certify
- Provide access to these activities

The Commission's role: (43(8)); (43(9)); see also Art 92, on the exercise of delegation

- May adopt delegated acts to specify the requirements for the certifications (43(8)); see also Art 92, on the exercise of delegation
- May adopt implementing acts laying down technical standards for certifications and mechanisms to promote or recognise certifications

II. Certification bodies in the framework of Article 43 GDPR

Certification bodies issue, renew and withdraw certifications: (43(1))

- Must have an appropriate level of data protection expertise
- DPAs have the power to disapprove or revoke individual certifications provided by certification bodies "where necessary" (See also 58(2)(h))
- Responsible for the assessment leading to certification or withdrawal of certification (43(4))
- Must provide to the competent DPAs the reasons for granting or withdrawing certifications (43(5))

Must be accredited by DPAs and/or national accreditation bodies: (43(1)(a) and (b), 43(3), 43(4); see also 64(1)(c); 57(1)(p); 70(1)(p))

- For a maximum of 5 years
- On the basis of accreditation criteria approved by the DPA or the EDPB
- (Separate requirements in the case of accreditation by a national accreditation body) (established according to Regulation 765/2008 (Accreditation Regulation))
- DPAs and EDPB must make public the accreditation criteria for CBs (and certification criteria) (46(6); see also 42(8) and 70(1)(o))
- The DPA or national accreditation body can revoke the accreditation of a CB (43(7))

Conditions for accreditation of CBs: (43(2))

- Demonstrate independence and expertise
- Undertake to respect the approved certification criteria

- Establish procedures for issuing periodic review and withdrawal of certification
- Establish transparent complaint-handling mechanisms
- Demonstrate absence of conflicts of interest

Appendix II -- Schematic Overview Certification Tasks and Actors

GDPR Certification Actors

Member States	DPAs	EDPB	Commission	Certification Bodies	National Accreditation Body	Private Sector Organizations
Encourage Certifications (42(1))	Encourage Certifications (42(1); 57(1)(n))	Encourage Certifications (42(1)); 70(1)(n)	Encourage certifications (42(1))	Issue/renew/withdraw certifications (42(5); 42(7); 43(1))	Accredit Certification Bodies (43(1)(b))	Draft/propose certification criteria and Mechanisms
Ensure that Certification Bodies are accredited (43(1))	Approve accreditation criteria for Certification Bodies (43(1)(b);(43(3); 64(1)(c); 57(1)(p))	Approve accreditation criteria for Certification Bodies (43(3)); 64(1)(c); 70(1)(p))	"lay down technical standards for cert. mechs. and mechs. to promote and recognize cert. mechs" (through implementing acts)(43(9)) [Create accreditation criteria for Cert. Bodies ?]			Provide input into creation of certification criteria
	Approve certification criteria (42(5); 43(2)(b); 57(1)(n))	Approve certification criteria (42(5); 43(2)(b)); 70(1)(q)(provide opinion to Commission)	Specify requirements for cert. mechs. (through delegated and implementing acts)(43(8) [Adopt certification criteria ?]			Become certified (and attendant tasks, such as providing information and access to Certification Bodies and enter into safeguards commitments with c-b parties) (42(6); 46(2)(f)
	Accredit Certification Bodies (43(1)(a); 43(7); 57(1)(q); 58(3)(e))	Accredit Certification Bodies (70(1)(o))				
	Publicize accreditation criteria and certification criteria (43(6))	Publicize in Register Certification Mechanisms (accredited certification bodies) and certified organizations in third countries (42(8); 43(6); 70(1)(o))				
	Issue/renew/withdraw certifications (42(5); 42(7); 43(1);57(1)(o); 58(1)(c) and (2)(h)); 58(3)(f))					

GDPR Certification Tasks

Encourage Certifications	Approve accreditation criteria for Certification Bodies	Ensure that Certification Bodies are accredited	Accredit Certification Bodies	Specify requirements for Cert Mechs and lay down technical standards for Cert Mechs and Mechs to promote and recognize Cert Mechs	Draft/Propose Certification Criteria/Mech	Approve/Adopt Certification Criteria/Mechanisms	Issue/renew/withdraw certifications to controllers or processors	Publicize accreditation criteria and certification criteria and mechs
DPAs (42(1); 57(1)(n))	DPAs (43(1)(b); 43(3); 64(1)(c); 57(1)(p))		DPAs (43(1)(a); 43(2); 43(7); 57(1)(q); (58)(3)(e)			DPAs (42(5); 43(2)(b); (57)(1)(n))	DPAs (42(5); 42(7); 43(1); 57(1)(o); 58(1)(c); 58(2)(h); 58(3)(f)	DPAs (43(6))
EDPB (42(1); 70(1)(n)	EDPB (43(3); 64(1)(c); (70)(1)(p);		EDPB (70(1)(o)			EDPB (42(5); 43(2)(b); 70(1)(q) (opinion to Comm.)		EDPB (42(8); 43(6); 70(1)(o)
Member States (42(1))		Member States (43(1))						
Commission (42(1);	Commission (through implementing acts) (43(9)) [?]			Commission (through delegated and implementing acts)(43(8) and (9)	Commission (through delegated or implementing acts) (43(8) and (9)) [?]	Commission (through delegated or implementing acts) (43(8) and (9) [?]; 92(3) and (5))		
	National Accreditation Bodies under Regulation (EC) No 765/2008 and specified technical rules (43)(3)		National Accreditation Body (43(1)(b))					
							Certification Bodies (with approval/input by the DPA) (42(5); 42(7); (43(1))	
					Private Sector			