

**Comments by the Centre for Information Policy Leadership****on the European Data Protection Board's****"Draft Guidelines 1/2018 on certification and identifying certification criteria in accordance with articles 42 and 43 of the Regulation 2016/679"****Adopted on 25 May 2018**

On 25 May 2018, the European Data Protection Board (EDPB) adopted its Draft Guidelines on certification and identifying certification criteria in accordance with articles 42 and 43 of the Regulation 2016/679 ("Draft Guidelines").<sup>1</sup> The EDPB invited public comments on this document by 12 July 2018.

The Draft Guidelines provide guidance on how to set up overarching criteria relevant to all types of certification mechanisms issued in accordance with article 42 (certification) and article 43 (certification bodies) of the General Data Protection Regulation (GDPR). The Draft Guidelines also contain an annex describing the list of tasks and powers of supervisory authorities in relation to certification in accordance with the GDPR.

The EDPB stated that it will publish at a later stage two separate sets of guidelines:

- (1) guidelines on identifying criteria to approve certification mechanisms as transfer tools to third countries or international organisations in accordance with article 42(2);<sup>2</sup>
- (2) guidelines for the supervisory authorities to assess certification criteria for the purpose of approval in order to ensure a harmonised approach. These guidelines will be made available at a later stage in an annex to the Draft Guidelines.<sup>3</sup>

The Centre for Information Policy Leadership (CIPL)<sup>4</sup> welcomes the opportunity to submit the comments below, both as input for the EDPB's final Guidelines ("Final Guidelines") and the two other upcoming guidelines mentioned above.

CIPL has already written extensively on certifications under the GDPR. Firstly, it published a white paper on Certifications, Seals and Marks under the GDPR and Their Roles as Accountability

---

<sup>1</sup> Draft Guidelines 1/2018 on certification and identifying certification criteria in accordance with articles 42 and 43 of the Regulation 2016/679, available at [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_1\\_2018\\_certification\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_1_2018_certification_en.pdf).

<sup>2</sup> Id. at page 4.

<sup>3</sup> Id. at page 7.

<sup>4</sup> CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 61 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

Tools and Cross-Border Data Transfer Mechanisms in April 2017 (“CIPL Discussion Paper”).<sup>5</sup> Secondly, in March 2018, it responded to the Article 29 Working Party’s (WP29) draft guidelines on the accreditation of certification bodies.<sup>6</sup> Both papers are attached as an annex to this document for reference. Finally, the importance of certifications as accountability tools and enablers of effective data protection and trust in the digital society will also be extensively discussed in two upcoming CIPL white papers on the central role of accountability in data protection and on how to incentivise accountability.<sup>7</sup>

### Comments

CIPL welcomes many of the clarifications provided by the Draft Guidelines as a basis for the future development of certifications under the GDPR. In particular, CIPL shares the EDPB’s views that (1) certifications could play an important role in the accountability framework for data protection,<sup>8</sup> (2) the Final Guidelines are to be used as a tool to help Member States, supervisory authorities and national accreditation bodies to establish a more consistent and harmonised approach for the implementation of certification mechanisms<sup>9</sup> and (3) certification criteria shall be interoperable with existing standards.<sup>10</sup>

As discussed in greater detail in CIPL’s earlier contributions on this topic, GDPR certifications are a promising instrument for data protection and will be important to both controllers and processors of all sizes. As stated in article 24(3) GDPR, certifications are intended to serve as an accountability tool that can be used to demonstrate compliance with the GDPR within the EU. In addition, under article 42(2) GDPR, they can also function as cross-border transfer mechanisms thereby implementing the EU Commission’s policy goal of working towards cross-border convergence.

To achieve these goals, CIPL believes that certification mechanisms should:

- Be based on a **harmonised EU-wide minimum GDPR certification standard** or template that is adaptable to different contexts;
- Be **flexible and scalable** to allow for a wide variety of certifications (including specific products, services and processes) to accommodate the differing size, scope, activity and needs of organisations of all sizes, consistent with the mandate in article 42(1);

---

<sup>5</sup> CIPL Discussion Paper on “Certifications, Seals and Marks under the GDPR and their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms”, 12 April 2017, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_gdpr\\_certifications\\_discussion\\_paper\\_12\\_april\\_2017.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf).

<sup>6</sup> CIPL comments on the Article 29 Data Protection Working Party’s “Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679”, 29 March 2018, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_comments\\_on\\_wp29\\_guidelines\\_on\\_accreditation\\_of\\_certification\\_bodies\\_under\\_the\\_gdpr.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_guidelines_on_accreditation_of_certification_bodies_under_the_gdpr.pdf).

<sup>7</sup> CIPL projects these papers will be released in early Fall 2018.

<sup>8</sup> Supra note 1 at page 2.

<sup>9</sup> Id. at page 3.

<sup>10</sup> Id. at page 16. In the current document, the terms “certification standards” and “certification criteria” are used interchangeably and should be understood as being equivalent in meaning.

- Permit the **certifying of entire organisational privacy management programs** (similar to Binding Corporate Rules (BCR)), in addition to specific products, services and processes;
- Enable **interoperability as much as possible** with other, similar EU accountability schemes as well as other certification schemes in other countries and regions and in particular the APEC Cross-Border Privacy Rules (CBPR) and APEC Privacy Recognition for Processors (PRP) (allowing companies to leverage compliance with other schemes to the extent their substantive and procedural requirements overlap with the GDPR certifications).<sup>11</sup>
- Be construed on the basis of a **holistic approach** which enables both national or EU compliance and cross border compliance as part of one set of certification criteria.

CIPL believes that the current version of the Draft Guidelines does not sufficiently address these overarching principles. In addition, CIPL believes that the Draft Guidelines are too limited in scope<sup>12</sup> in that they refer to subsequent guidelines to address topics that should be integrated in the current document to accelerate the creation of, and provide further clarity on, a GDPR certification framework. Setting up this framework to enable the consistent development of diverse but interoperable accountability and transfer tools should be a top priority of the EDPB as it fosters compliance with the GDPR and other applicable privacy laws. CIPL therefore recommends that the EDPB include in the Final Guidelines a short and clear timeline for the adoption of a comprehensive EU-wide minimum GDPR certification standard (covering all elements of the GDPR) to be put in place before other more narrow and specialised certifications may be approved on the basis of the EU-wide standard.

Moreover, in CIPL's view, it is also crucial that the European Commission adopts delegated and implementing acts under articles 43(8) and (9) as soon as possible. The EDPB should encourage the Commission to do so. CIPL advises including such encouragement in the Final Guidelines.

The Draft Guidelines rightfully explain that certification criteria must be developed, approved and published before a certification can be issued to and used by an organisation.

CIPL believes that, at the outset, the Draft Guidelines should provide a preliminary list of definitions to clarify the notions of a "certification scheme", "certification criteria", "certification mechanism", "certification procedure", "certification Target of Evaluation (ToE)", "certification owner" and "scheme owner".

In addition, due to the complexity of the certification process and the numerous stakeholders it involves, CIPL recommends that the EDPB provide an example or illustration that would summarise the process at a glance — from the submission of the application stage to the final sign-off stage — for different organisations. In particular, it would be helpful if the EDPB could provide an illustration of the process required for each of the following (i) becoming a

<sup>11</sup> See APEC CBPR and PRP system documents, available at <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>. The APEC CBPR and PRP have emerged as a significant accountability and cross-border transfer frameworks in the Asia-Pacific region (See [www.cbprs.org](http://www.cbprs.org)).

<sup>12</sup> Supra note 1 at page 3.

certification body, (ii) receiving approval for a certification scheme and (iii) becoming a certified organisation.

CIPL takes this opportunity to provide recommendations for consideration when drafting the final version of the Draft Guidelines, including reiterating some of the key points previously made in the CIPL Discussion Paper.

In the comments below, CIPL highlights:

- (1) the need to develop an EU-wide baseline GDPR certification standard as a necessary first step in the process of creating a well-functioning certification system in the EU;
- (2) the need to enable the certification of a privacy management program as a whole, similar to BCR;
- (3) the urgent priority that should be given to developing globally interoperable GDPR certification mechanisms to be used as transfer tools to third countries or international organisations.

## **I. Development of the Certification Criteria**

As noted in the CIPL Discussion Paper, to facilitate EU-wide harmonisation and global interoperability, there should be one common EU certification baseline standard to be used for all contexts and sectors.<sup>13</sup> This baseline standard will enable both EU-wide general GDPR certifications as well as more narrow GDPR certifications customised for specific products, services, processes, industry sectors and/or jurisdictions. This EU-wide baseline standard should be developed by the European Commission and/or the EDPB in collaboration with certification bodies and industry. This approach is necessary to ensure consistency and harmonisation between certifications and to avoid unnecessary overlap and proliferation of certifications that could lead to confusion for stakeholders and an inability to create interoperability with other non-EU certification and transfer schemes. Such an approach also ensures that organisations see the value in seeking GDPR certifications.

### **A. Scope of the Certification**

#### **1. Material Scope**

The Draft Guidelines acknowledge that the GDPR provides a broad scope for what can be certified and that several components of the GDPR are relevant for the design of certification procedures and criteria, but that depending on the object of the certification some elements may be disregarded and not be taken into account if they are not relevant to the object of certification.<sup>14</sup>

This approach aligns with CIPL's previous recommendations on the scope of certifications<sup>15</sup> in that (1) the certification of a whole organisation's privacy management program should be

---

<sup>13</sup> Supra note 5 at page 9.

<sup>14</sup> Supra note 1 at page 11.

<sup>15</sup> Supra note 5 at page 9.

possible<sup>16</sup> and (2) certification criteria should be both comprehensive and flexible in order to provide for industry and sector-wide consistency at the EU level while allowing for specific adaptation and application by certification bodies to take into account the nature of a business sector, company, product, service or process. The availability of a wide range of certifications — from comprehensive to those with a narrower scope — would promote the use of certifications by ensuring that a wide cross-section of controllers and processors have access to a certification mechanism appropriate to their business needs.

In order to achieve this, CIPL recommends the development of baseline certification criteria or standards that may subsequently be implemented through a gating methodology to identify the criteria relevant to a particular case. If a criterion does not apply to the certification applicant's specific case, the certification assessment would continue on the basis of the remaining criteria.<sup>17</sup> This method would help structure and streamline the certification process while allowing for replicability and interoperability. As further explained in Section VII of this document, this method will be useful to identify at an early stage if the certification is local or is also to be used as an international transfer mechanism. This could be determined efficiently at the outset by having the applicant answer a question around whether the certification is intended to serve as an international transfer mechanism.

## 2. Geographic Scope

CIPL has previously recommended that, in accordance with article 42(1), GDPR certification mechanisms should be based on EU-wide baseline certification criteria to avoid national fragmentation.<sup>18</sup> This EU-wide baseline would enable both national and EU-wide certifications to work in parallel while ensuring consistency, replicability and interoperability as follows:

- EU-wide certifications that may result in a European Data Protection Seal<sup>19</sup> covering all Member States are based on the EU-wide certification baseline standard approved by the EDPB and/or the Commission.<sup>20</sup> The Draft Guidelines provide that the mechanism for the European Data Protection Seal and its criteria should take into account national sector specific regulations and shall envisage an EU-wide application.<sup>21</sup> While CIPL fully agrees with the need for EU-wide application and the advantages of taking existing national practices into account, CIPL emphasises that national sector specific provisions should not be taken into account *a priori*. Indeed, it would be impossible and counter-productive to take all actual and potential national sector-specific requirements into account at the outset. Instead, the EU-wide baseline certification standard would be based exclusively on the GDPR and should be drafted in a way that makes it customisable for jurisdiction- sector- product- and process-specific requirements, as necessary and appropriate.

---

<sup>16</sup> Id. at page 7.

<sup>17</sup> In practical terms that would translate into a questionnaire stating that “if question X is not relevant, please go directly to question Y”. For example, if the organisation is only applying for a local certification, the criteria related to cross-border transfers should be disregarded and the question as to whether the organisation will be using the certification as a cross-border transfer mechanism should be skipped.

<sup>18</sup> Supra note 5 at page 9.

<sup>19</sup> See article 42(5) GDPR and Supra note 1 at page 9.

<sup>20</sup> See articles 43(8) and 43(9) GDPR.

<sup>21</sup> Supra note 1 at page 10.

- National certifications<sup>22</sup> — whether current or future — should be similarly aligned with the common EU-wide EDPB approved certification baseline standard, including certifications that may already be under development in the Member States. Such a baseline should be used as a reference by certification owners, organisations and supervisory authorities when developing certification criteria and by the supervisory authorities when approving certification criteria for the issuance of national certifications. When certification criteria are available at the EU level, there should be no possibility to have certifications criteria developed at national level independently or in isolation without taking into consideration first the EU-wide certification baseline. When such national certification criteria are adopted they should only address specific national or sector specific requirements that are not already taken into consideration at the EU level.

## **B. Who Should Develop the Certification?**

CIPL welcomes the acknowledgement by the Draft Guidelines that the supervisory authority may, in addition to creating its own certification scheme, encourage the market to develop certification mechanisms<sup>23</sup> (however, such certifications should be modelled on a pre-existing EU-wide GDPR certification standard, as discussed above). Therefore, the EDPB and supervisory authorities should explicitly state that they are open to endorsing certification mechanisms developed by private sector stakeholders — whether these comprise existing mechanisms or standards or new ones still to be developed. This will encourage and incentivise the market to develop certifications.

Furthermore, in cases where supervisory authorities (or other public bodies) seek to develop certification standards, the development of such certification criteria should be a multi-stakeholder process involving private sector organisations such as certification bodies and businesses.<sup>24</sup> As certifications must work in practice within the various business contexts for which they are designed, the experience and know-how of these stakeholders is essential to the development of viable certifications.

In addition, CIPL calls for regular communication between industry, the EDPB, supervisory authorities, the Commission, certification and accreditation bodies, following structured consultation procedures. Such procedures should preferably be carried out by the EDPB and the Commission in line with articles 42(1) and 70(1)(n)<sup>25</sup> of the GDPR.

CIPL wishes to underline the urgency to work on the criteria since as of today no other work on certifications can commence pending the issuance and adoption of certification criteria in the form of an EU-wide certification standard.

---

<sup>22</sup> National certifications should be used only for organisations whose privacy programs, services and products are limited to a single Member State.

<sup>23</sup> Supra note 1 at page 6.

<sup>24</sup> Supra note 5 at page 15.

<sup>25</sup> Article 70(1)(n) GDPR gives the board the task to encourage the establishment of data protection certification mechanisms and data protection seals and marks.

## **II. Approval of the Certification Criteria**

As already explained, when the EDPB or supervisory authorities approve criteria relevant to certification mechanisms, the preference should be that they do so under a common EU-wide certification standard approved by the EDPB. This would be in line with articles 42(5), 58(3)(f) and 63 of the GDPR.

The announced guidelines of the EDPB for the supervisory authorities to assess certification criteria for approval in order to ensure a harmonised approach should not be framed as guidelines but as an actual EU-wide baseline standard against which future more narrow GDPR certifications can be assessed. Such standards or specific criteria are necessary to provide sufficient detail for supervisory authorities to assess and approve certifications in a way that ensures sufficient consistency and harmonisation between different certifications.

## **III. Publication of the Approved Certification Criteria**

According to article 43(6) GDPR, approved certification criteria shall be made public by the supervisory authorities and transmitted to the EDPB who shall then collate them and make them publicly available in a register.

Having all certifications mapped against the EU-wide certification standard would definitely help in ensuring better readability of the register as well as understanding various certifications' scope and facilitate their interoperability with other GDPR certifications (because all of them will have been evaluated and approved on the basis of the same baseline standard). This transparency is required both for individuals<sup>26</sup> and businesses. More specifically, this would also enable companies that are certified in one Member State to understand and identify potential synergies and bridges to become certified in other Member States or at EU level and would help in encouraging a mutual recognition process between national certifications. In summary, it will be easier for the EDPB to publish approved certification criteria by supervisory authorities in a harmonised, consistent and transparent manner if these certifications were based on an EU-wide certification standard.

## **IV. Certification of the Organisation on the Basis of Approved Certification Criteria**

The GDPR allows for the certification of organisations either by supervisory authorities or by certification bodies that will have to rely on similar methods to assess the fulfilment of certification criteria by the applicant organisation.

### **A. Certification by a Supervisory Authority**

CIPL welcomes the acknowledgment in the Draft Guidelines that when acting as a certification body, a supervisory authority's role should be transparent in the exercise of its functions and it must give careful consideration to the separation of powers relating to investigations and

---

<sup>26</sup> Recital 100 of GDPR provides that in order to enhance transparency and compliance with the Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.



enforcement to avoid any potential conflict of interest.<sup>27</sup> As previously stated in the CIPL Discussion Paper, in general, for efficiency and scalability reasons, CIPL expresses a preference for third-party certification by certification bodies over certification by supervisory authorities as it protects the supervisory authorities' functional independence.<sup>28</sup>

#### **B. Certification by a Certification Body**

CIPL would like to underline that at this stage, unfortunately, no certification body can issue certifications. To become a certification body, the organisation must be accredited from either the competent supervisory authority or the national accreditation body.<sup>29</sup> Where the accreditation is handled by the national accreditation body, it must be done in accordance with EN-ISO/IEC 17065/2012 and the additional requirements established by the competent supervisory authority.<sup>30</sup> Based on the above, it appears that no certification body can apply for accreditation until the supervisory authorities have set and published their additional requirements. CIPL would like to highlight that absent the publication of these requirements, certifications cannot be issued by bodies other than the supervisory authorities themselves. As a result, the implementation of accountability tools that companies are eager to use is indefinitely delayed. The EDPB should encourage supervisory authorities to define these rules as soon as possible, including guidance to apply for accreditation and submit a certification scheme for approval. CIPL recommends such accreditation standards reflect CIPL's recommendations on the WP29's draft guidelines on the accreditation of certification bodies.<sup>31</sup>

In addition, the EDPB should recommend that each supervisory authority maintain an up-to-date register of accredited certification bodies and the type and scope of certification they can issue. This would enable any certification applicant to easily identify the approved certification bodies in a reliable manner.

#### **C. Assessment Methods of the Applicant**

While assessment methods used by different certification bodies and supervisory authorities across the EU should be streamlined and equivalent, CIPL would like to raise a concern related to methods of verification and compliance checks (such as onsite inspections or requests for extensive documentation) that may run afoul of the legitimate business needs related to confidentiality or the protection of intellectual property or trade secrets.

The certification process should not be too burdensome and intrusive on organisations so as not to discourage them from seeking certifications. Their voluntary nature must be taken into account, and every effort should be made to encourage the emergence of these mechanisms. Therefore, the EDPB should acknowledge that the certification process can take various forms, and that proof of compliance can be provided through mechanisms which are not too onerous.

---

<sup>27</sup> Supra note 1 at page 6.

<sup>28</sup> Supra note 5 at page 15.

<sup>29</sup> See article 43(1) GDPR.

<sup>30</sup> Similarly, the WP29 draft guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679 mentions that if accreditation is offered by the competent supervisory authority, a certification body applying for accreditation will have to meet the requirements set by the respective supervisory authority.

<sup>31</sup> Supra note 6.



## V. Certification as an Aggravating Factor

The Draft Guidelines rightly mention that certification mechanisms are entirely voluntary and designed to “assist in demonstrating compliance”.<sup>32</sup> In order to encourage the development of these mechanisms as an accountability tool, companies have to be incentivised to make the necessary investments.<sup>33</sup> As a result, CIPL disagrees with the suggestion by the EDPB that certifications can be used as a potential “aggravating or mitigating factor” for a supervisory authority when deciding to impose a fine.<sup>34</sup> CIPL recommends that this statement be further clarified to say that certifications can be used principally as a mitigating factor, except in cases of repeated or serious violations of the certification criteria or in cases of misrepresentation related to the certification, in which case such malfeasance might be used as an aggravating factor. In addition, if a fine is being considered under article 83(2) for non-compliance with a provision of the GDPR that is unrelated to the object of the certification, such certification should not be used as an aggravating factor against the organisation.

## VI. The Certification of a Privacy Management Program

CIPL has already supported the need for programmatic certifications and pointed to BCR as a possible benchmark to further develop such certifications.<sup>35</sup>

### A. The Need for Programmatic Certification

In Section 1.2, the Draft Guidelines indicate that the GDPR defines the context surrounding the use of certification mechanisms as an element to demonstrate compliance with specific obligations of controllers and processors.<sup>36</sup> CIPL would like to stress that there are many specific obligations in the GDPR that can have differing scope, from the smallest (at process or product level) to the widest (at organisation level). Of course, article 25 (data protection by design and by default) and article 32 GDPR (security of processing) both refer to certification mechanisms relating to their respective scope,<sup>37</sup> but this should not be understood as precluding the use of certification mechanisms as an element to demonstrate compliance with a wider scope.

Equally, the notions of “product”, “service”, “system” “operation” or “processing operation” used in articles 42 and 43 of the GDPR should be interpreted as including the certification of a comprehensive privacy management program. In particular, a system refers to processing operations that may relate to an entire privacy program. The EDPB’s Final Guidelines on certification should clarify this point so as not to reduce the scope and flexibility offered by certifications as a compliance tool.

---

<sup>32</sup> Supra note 1 at page 3.

<sup>33</sup> Supra note 5 at page 7.

<sup>34</sup> Supra note 1 at page 3 (emphasis added).

<sup>35</sup> Supra note 32.

<sup>36</sup> Supra note 1 at page 4 (emphasis added).

<sup>37</sup> See article 25(3) for an approved certification mechanism to be used as an element to demonstrate compliance with the data protection by design and by default requirements set out in article 25(1) and 25(2) of the GDPR. See article 32(3) for an approved certification mechanism to be used as an element to demonstrate compliance with the security requirements set out in article 32(1) of the GDPR.

Articles 24(3) and 28(5) of the GDPR — also mentioned by the Draft Guidelines — support the application of certification mechanisms at a programmatic level. Article 24(1) mandates that the controller, on the basis of risk, implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. The same wording applies in article 28(4) as it relates to processors. Since they require the setting up of a governance structure, the adoption and implementation of policies, the training of employees and the introduction of appropriate controls, such technical and organisational measures trigger the implementation of a comprehensive privacy program. This is all the more necessary since article 24(1) provides that technical and organisational measures shall be reviewed and updated where necessary. This review and updating is most efficient when performed as part of an existing privacy program with relevant procedures in place. Depending on the size, risk profile and business sector of the organisation, such measures can be defined at different levels of granularity, i.e., at the product or processing level, or at a particular business unit or department level, or at a country or regional level or even at a global level, covering all business units and departments.

The Draft Guidelines describe the components that have to be considered when assessing a processing operation (personal data, systems, processes and procedures).<sup>38</sup> The EDPB recognises that the scope of certification is directed to “processing operations or sets of operations”,<sup>39</sup> including governance processes understood as organisational measures. When these “processing operations or sets of operations” are defined at the level of a company or a group of companies, that opens up the possibility to certify an entire privacy program. Thus, CIPL urges the EDPB to clarify that its analysis in the Draft Guidelines is consistent with and supports the creation of programmatic certifications.

Conversely, CIPL believes that there should be no inference that the programmatic nature of the certification would reduce compliance at a more granular level (for instance at the product or service level) as effective operational compliance depends primarily on the nature, scope, calibration and effectiveness of controls in place.

In the end, allowing for programmatic certification may foster better compliance as it enables organisations to extend the scope of their certification in a mutualised and pragmatic manner at once, instead of having to apply for many different certifications with varying scopes and a myriad of different stakeholders and certification schemes, in particular if they operate across different countries.

Programmatic certifications also enable and, indeed, are a prerequisite for potential interoperability with other accountability tools such as BCR or non-EU certifications such as the Privacy Shield or APEC CBPR and PRP.

## **B. BCR as the Certification of a Privacy Management Program**

BCR have been codified as an international transfer mechanism in article 47 GDPR. CIPL has long explained that BCR are first and foremost the formalisation of a privacy program and are as such an accountability tool<sup>40</sup> in addition to serving as a basis for international transfers. This position

---

<sup>38</sup> Supra note 1 at page 11.

<sup>39</sup> Id. at page 12.

<sup>40</sup> Supra note 5 at page 12.

has also been formally recognised by the WP29.<sup>41</sup> As required by article 47 GDPR and explained in the WP29 Working Documents WP256 and WP257,<sup>42</sup> BCR must contain governance, policies, processes, guidelines and practical tools to ensure effective implementation of the general data protection principles, of the rights of data subjects, of liability and transparency, as well as procedures on audit, reporting and cooperation with the supervisory authority. The implementation of this privacy program throughout the organisation is the necessary prerequisite for enabling international transfers of personal data across the organisation. Transfers may take place because a privacy program which ensures an adequate level of protection has been put in place throughout the company. The legal basis for data transfers is a direct result of the establishment of a company-wide privacy program such as BCR.

Application for BCR approval is made to the supervisory authority that is responsible for the proper assessment of the draft BCR of the applicant, leading to the approval of the BCR, in line with the consistency mechanism.<sup>43</sup> The process for BCR approval is very similar to that of a certification as applicant companies must demonstrate to the supervisory authority and EDPB that their BCR provide adequate safeguards to protect personal data throughout their organisation in line with the requirements of article 47 GDPR, as explained in Working Documents WP256 and WP257. Thus, the supervisory authority and EDPB, tasked with verifying that the requirements are fulfilled by the BCR applicants,<sup>44</sup> are acting like a certification body issuing a certification. The definition of certification in the Draft Guidelines<sup>45</sup> as third-party attestation related to processing operations by controllers and processors, in fact, describes not only the certification process but also accurately reflects the BCR approval process.

BCR predated GDPR and companies voluntarily submitted to higher standards. Investments made by BCR-approved organisations should be recognised as a certification to ensure that companies do not have to go through an unnecessary certification process again. If BCR are not recognised as a certification in the sense of article 42 GDPR, at minimum they should be recognised as being substitutable and interoperable with certifications. The CNIL already recognises BCR as an accountability mechanism interoperable with certifications. When companies receive approval for their BCR, the CNIL certification department contacts them to provide further information on the accountability tools that are offered by the CNIL and remind

---

<sup>41</sup> BCR have already been recognised as an accountability demonstration mechanism by the WP29 as early as 2010 in its Opinion WP 173-3/2010 on the principle of accountability. Paragraph 19 provides that “binding corporate rules (“BCRs”), which are used in the context of international data transfers, reflect the accountability principle. Indeed BCRs are codes of practice, which multinational organisations draw up and follow, containing internal measures designed to put data protection principles into effect (such as audit, training programmes, network of privacy officers, handling complaint system). Once reviewed by national data protection authorities, BCRs are deemed to ensure adequate safeguards for transfers or categories of transfers of personal data between companies that are part of the same corporate group and that are bound by these corporate rules”.

<sup>42</sup> WP256 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules [https://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48798](https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798) and WP257 Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules [https://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48799](https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48799).

<sup>43</sup> See article 64 (1)(f) GDPR.

<sup>44</sup> See article 47 (1) GDPR.

<sup>45</sup> Supra note 1 at page 5.

them of the additional criteria they need to fulfil in order to be eligible for particular certification as many requirements of said certification are already fulfilled by the BCR.

Moreover, CIPL suggests that the BCR referentials could serve as a good basis for developing an EU-wide certification baseline. BCR have proven to be efficient and so far 130 companies are now “BCR certified”. The Working Documents WP256 and WP257 fulfil the requirement that certification criteria be clear and comprehensible and that they allow for practical application. The documents also already include the compliance aspects to be taken into account when certification criteria are drafted.<sup>46</sup>

Finally BCR should be further leveraged in the creation of the criteria for approving certification mechanisms as international transfer tools as they are both an accountability tool approved by the EDPB and an international transfer tool.

CIPL recommends the EDPB include a section in the Final Guidelines on the relationship between GDPR Certifications and BCR, in line with the above.

## **VII. Certification as International Transfer Tools**

As previously mentioned in the CIPL Discussion Paper, any guidelines on the identification of criteria to approve certification mechanisms as international transfer tools should: (1) leverage existing mechanisms such as BCR; (2) consider the EU Commission’s policy goal of working towards cross-border convergence and interoperability with respect to similar transfer mechanisms;<sup>47</sup> and (3) draw guidance from the APEC CBPR and PRP system documents.<sup>48</sup> As explained before, CIPL calls for these guidelines<sup>49</sup> to be issued as a matter of priority to facilitate international data transfers and in any event should be part and parcel of the EU-wide baseline certification standard.

As already explained in this paper, in the interests of consistency and streamlining, certification and international transfer criteria should be addressed as part of the same process: the international transfer component of a certification could very well be managed as part of the certification criteria themselves with the relevant criteria to be added and managed on the basis of a gating procedure including specific questions on international transfers.<sup>50</sup> As a matter of fact, example 5 provided in Section 6.2 of the Draft Guidelines<sup>51</sup> on certification relating to cloud computing integrates this approach as it already includes the international transfer component of the service (servers located outside of the EU) and the need for the criteria to take into account the requirements of Chapter V of the GDPR with respect to data transfers to third countries. Therefore, if a cloud service complies with the certification criteria, it will be certified

---

<sup>46</sup> See pages 10 and 11 of the Draft Guidelines that contain the same requirements as WP256 and WP257.

<sup>47</sup> 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](http://ec.europa.eu/newsroom/document.cfm?doc_id=41157).

<sup>48</sup> Supra note 11.

<sup>49</sup> As with the other announced guidelines, CIPL believes the guidelines on identifying criteria to approve certification mechanisms as transfer tools to third countries or international organisations should not be framed as guidelines but rather as an actual EU-wide baseline standard (see discussion on page 7 above).

<sup>50</sup> See discussion on pages 4 and 5 above.

<sup>51</sup> Supra note 1 at page 17.

as both a GDPR-compliant service in itself, and also as compliant with the GDPR rules on international transfers. The same approach should be developed with respect to all objects of certification under article 42.

In addition, this approach is already applicable as regards the BCR as only a few elements of the BCR referential actually relate to international transfers. The majority of the criteria required for BCR approval relate to programmatic requirements such as governance, privacy policies, audit, security, privacy office organisation, data subject rights, and duty to collaborate, that are applicable to all Group entities regardless of where they are located (inside or outside of the EU).

Furthermore, the requirements of article 42(2) for controllers and processors not subject to GDPR to make binding and enforceable commitments to apply the appropriate standards required by law could be based on the instruments used under the BCR.<sup>52</sup>

Finally, the EDPB and the Commission should clarify that certified products, services and programs should be interoperable with other global certification schemes, such as the Privacy Shield or the APEC CBPR and PRP and that any certification criteria should maximise the potential interoperability with similar scalable certification schemes around the world. “Interoperable” should be understood as meaning that companies having processes, mechanisms and documentation in place allowing them to be certified under the GDPR shall be enabled to leverage that certification for getting certified or approved under another system to the extent of their common requirements, and *vice versa*. This enables companies not to re-certify to the same obligations over and over but to focus on any additional requirements not already covered by their existing certification. For example, the EDPB should encourage that elements of certification provided for the purpose of CBPR certification should be accepted under the EU scheme to the extent that they are essentially equivalent and not undergo renewed and duplicative review and assessment.

### **Conclusion**

CIPL is grateful for the opportunity to provide comments on key implementation questions on certification and identifying certification criteria in accordance with articles 42 and 43 of GDPR. We look forward to providing further input as the relevant standards are being developed, as well as to contributing generally to the development of effective, interoperable and scalable GDPR certifications.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, [bbellamy@huntonAK.com](mailto:bbellamy@huntonAK.com), Markus Heyder, [mheyder@huntonAK.com](mailto:mheyder@huntonAK.com), Nathalie Laneret, [nlaneret@huntonAK.com](mailto:nlaneret@huntonAK.com) or Sam Grogan, [sgrogan@huntonAK.com](mailto:sgrogan@huntonAK.com).

---

<sup>52</sup> Companies applying for BCR have the obligation to make them enforceable within their group of companies. See WP264 Section 4 providing examples to evidence how BCRs are made binding upon the members of the Group: Measures or rules that are legally binding on all members of the Group; Contracts or intra-group agreement between the members of the Group; Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the Group.

# ANNEX

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.<sup>1</sup> This is the fourth white paper in this series, following earlier CIPL papers on DPO, Risk, and OSS and Lead Authority.<sup>2</sup>

### 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<sup>3</sup> in a way that is pragmatic and benefits all stakeholders.<sup>4</sup>

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'

---

<sup>1</sup> See [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_gdpr\\_project\\_work\\_plan\\_17\\_march\\_2017.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_work_plan_17_march_2017.pdf)

<sup>2</sup> 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/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_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](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf)

<sup>3</sup> See Appendixes I and II for a summary of the GDPR certification provisions.

<sup>4</sup> 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.<sup>5</sup> 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.

---

<sup>5</sup> 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<sup>6</sup> and information management infrastructure, or the full range of an organisation’s products and services.<sup>7</sup> 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

---

<sup>6</sup> 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.

<sup>7</sup> 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.<sup>8</sup> 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:

---

<sup>8</sup> 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 discourage 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<sup>9</sup> 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.

---

<sup>9</sup> 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 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.”<sup>10</sup> 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

---

<sup>10</sup> 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](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.<sup>11</sup> 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.

---

<sup>11</sup> 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	DPA's	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
DPA's (42(1); 57(1)(n))	DPA's (43(1)(b); 43(3); 64(1)(c); 57(1)(p))		DPA's (43(1)(a); 43(2); 43(7); 57(1)(q); (58)(3)(e))			DPA's (42(5); 43(2)(b); (57)(1)(n))	DPA's (42(5); 42(7); 43(1); 57(1)(o); 58(1)(c); 58(2)(h); 58(3)(f))	DPA's (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			

**Comments by the Centre for Information Policy Leadership**

**on the Article 29 Data Protection Working Party's**

**"Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679"**

**adopted on 6 February 2018**

On 6 February 2018, the Article 29 Data Protection Working Party (WP) adopted its Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679 (Draft Guidelines).<sup>1</sup> The WP invited public comments on this document by 30 March 2018.

The Draft Guidelines provide guidance on how to interpret and implement Article 43 (certification bodies) of the GDPR, focussing mainly on the applicable standards for both National Accreditation Bodies (NABs) and Supervisory Authorities (SAs) for accrediting certification bodies under Article 43.1. The Draft Guidelines also envision an Annex containing a more detailed "framework for identifying accreditation criteria [for certification bodies]".<sup>2</sup> The WP has noted that the Annex will be prepared at a later stage to "take into account comments submitted in the framework of the ongoing public consultations".<sup>3</sup>

The Centre for Information Policy Leadership (CIPL)<sup>4</sup> welcomes the opportunity to submit the comments below, both as input for the WP's final Guidelines and the content of the Annex to the Guidelines. Following CIPL's 12 page submission, we attach the APEC Accountability Agent recognition criteria for the CBPR and PRP systems (see Annex) which could be instructive in any process of developing an EU-wide accreditation standard for certification bodies certified by SAs.

---

<sup>1</sup> WP261 Article 29 Working Party Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679, [http://ec.europa.eu/newsroom/article29/document.cfm?doc\\_id=49877](http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877).

<sup>2</sup> See Footnote 1, at page 12.

<sup>3</sup> See WP announcement regarding public consultation deadline at [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=614486](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614486).

<sup>4</sup> CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 59 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton & Williams.



As discussed in greater detail in CIPL's earlier white paper on this topic,<sup>5</sup> GDPR certifications will be important to both controllers and processors of all sizes. They can be used to demonstrate compliance with the GDPR within the EU, function as cross-border transfer mechanism under the GDPR and enable "interoperability" with other, similar certifications and accountability schemes in other countries and regions. CIPL's white paper on certifications also noted that certification mechanisms should be based on a harmonised EU-wide minimum certification standard or template that is flexible and adaptable to different contexts, as well as scalable to organisations of all sizes, consistent with the mandate in Article 42(1). How certification bodies are accredited under the GDPR is directly relevant to this issue.

CIPL underlines that the GDPR provides for more than one route towards an appropriate accreditation standard: one that builds on an existing system of NABs that operate under established ISO standards, and one for SAs allowing for greater flexibility. The availability of more than one system reflects the need for scalability, which is a key requirement for the accountability mechanisms in the GDPR. Accreditation by NABs will be particularly attractive for larger organisations which are used to working with certifications in various contexts, whereas accreditation by SAs will make accreditations and certifications more broadly accessible to micro, small and medium-sized enterprises.

Accreditations by SAs are new in the GDPR. Their success depends on the following critical factors:

- SA accreditation should be based on an appropriate EU-wide baseline accreditation standard or template to avoid national fragmentation;
- The EU-wide baseline accreditation standard or template may "be guided by" but should not have to strictly follow the ISO 17065 standard; and
- The standard should maximise the potential interoperability with similar scalable certification schemes around the world.

CIPL believes that both routes towards accreditation of certification bodies will have useful roles to play within their respective areas of core competency without compromising functional consistency between them, as further explained below.

Thus, with a few clarifications as suggested below, we believe that the Draft Guidelines may facilitate the creation of effective and widely used GDPR certifications.

---

<sup>5</sup> CIPL Discussion Paper on "Certifications, Seals and Marks under the GDPR and their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms", 12 April 2017, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_gdpr\\_certifications\\_discussion\\_paper\\_12\\_april\\_2017.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf).

### **Summary of CIPL Recommendations**

- When SAs accredit certification bodies pursuant to Article 43.1(a), the preference should be that they do so under a common EU-wide accreditation standard approved by the EDPB, taking into account, where relevant, the requirements adopted by the Commission in accordance with Article 43(8) GDPR.
- The EDPB should establish independent assessment criteria for reviewing SA-submitted accreditation criteria to maintain comparability and consistency across the EU, in line with Article 70(1)(o) GDPR.
- SAs and/or the EDPB and/or the Commission should not be required to strictly follow ISO 17065 as they develop or approve accreditation requirements for certification bodies under Article 43 GDPR. ISO 17065 should be viewed as instructive and useful for guidance, but not mandatory.
- The APEC Accountability Agent<sup>6</sup> Recognition Criteria are a good model for consideration in connection with accreditation standards to be developed by the SAs, the EDPB or the Commission.
- The forthcoming Annex to the accreditation guidelines (announced by the Draft Guidelines) setting forth guidelines on “how to identify additional accreditation criteria” should: (1) bear in mind the need for flexibility and scalability in light of the relevant GDPR mandate as discussed in CIPL’s comments; (2) consider the EU Commission’s policy goal of working towards cross-border convergence and interoperability with respect to similar transfer mechanisms; and (3) take guidance from the APEC Accountability Agent Recognition Criteria.
- When considering to what extent the ISO standard should “guide” the accreditation standards developed by the SAs and EDPB, relevant international experience dealing with certifications under ISO conformity assessments should be considered where the ISO standards have failed to ensure scalability and affordability for purposes of micro, small and medium-sized enterprises.
- The ISO 17065 standard should also be applied flexibly by the NABs to further the scalability goals of the GDPR with respect to micro, small and medium-sized enterprises and to facilitate consistency with the standard(s) developed or approved by the SAs or the EDPB or the Commission.
- The “additional requirements” the SAs develop for accreditations by NABs under Article 43.1(b) should also take into account scalability and the needs of micro, small and medium-sized enterprises.

---

<sup>6</sup> The term “Accountability Agents” in the APEC CBPR and PRP systems refers to the third-party certification organisations that provide CBPR or PRP certifications to companies.

## **Discussion**

### **I. Key GDPR provisions**

The GDPR certification scheme requires the existence of certification bodies that have been formally accredited to issue certifications to organisations. According to Article 43.1(a) and (b), certification bodies may be accredited by:

- (1) the competent supervisory authority (SA);
- (2) the national accreditation body (NAB); or
- (3) by both.<sup>7</sup>

Article 43.1(b) provides that the NABs<sup>8</sup> must accredit certification bodies “in accordance with EN-ISO/IEC 17065/2012 (ISO 17065) and with additional requirements established by the supervisory authority which is competent pursuant to Article 55 and 56” (Emphasis added).<sup>9</sup>

The GDPR does not require the SAs to rely on ISO 17065 when they accredit certification bodies; such requirement is only for NABs. Nor does the GDPR otherwise define a specific standard to be employed by the SA during the accreditation process, other than a list of general criteria for certification bodies in Article 43.2 that apply to accreditation by both an SA or an NAB. These criteria include independence, subject matter expertise, having approved certification criteria and procedures, and an absence of a conflict of interest.

Article 43.3, read together with Article 64.1, provides that accreditation of certification bodies by an SA shall take place on the basis of criteria approved by that SA, subject to an opinion by the EDPB, or by the EDPB itself pursuant to Article 63 (consistency mechanism). Article 43.3 also reiterates that accreditation of certification bodies by NABs shall be based on the criteria approved by the SA,<sup>10</sup> which will complement the requirements envisaged in Regulation (EC) No. 765/2008 and the ISO 17065 standards (i.e. “the technical rules that describe the methods and procedures of the certification bodies”, Art. 43.3).<sup>11</sup> However, as noted, the accreditation by SAs does not have to be in accordance with ISO 17065. As such, SA accreditations can be more flexible in their requirements and criteria than NAB accreditations.

---

<sup>7</sup> See Footnote 1, at page 8.

<sup>8</sup> NABs must also be “named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council” setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218/30. Article 43.1(b).

<sup>9</sup> See Footnote 1, at page 9.

<sup>10</sup> The phrase “those requirements” in Article 43.3 refers to the criteria developed by the supervisory authorities and the requirements set out in Article 43.2. Draft Guidelines, p. 9.

<sup>11</sup> See Footnote 1, at Section 4.3, page 9.

## II. Purpose of the Draft Guidelines

Noting the important role certifications can play to “enhance compliance with the GDPR and transparency for data subjects and in B2B relations, for example between controllers and processors”, the WP states that the purpose of the Draft Guidelines is “to provide guidance on how to interpret and implement the provisions of Article 43 of the GDPR” and to “help Member States, supervisory authorities and national accreditation bodies establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR”.<sup>12</sup>

The Draft Guidelines address several issues, two of which<sup>13</sup> will be the focus of CIPL’s comment:

- (1) providing a framework for establishing the “additional” accreditation requirements (in addition to ISO 17065) under Article 43.1(b) when the accreditation is handled by a NAB; and
- (2) providing a framework for establishing accreditation requirements for when the accreditation is handled by the SA.

## III. Scalability as an overarching requirement of GDPR certifications

The overarching question in this context is to what extent the applicable accreditation criteria for certification bodies facilitate the GDPR’s mandate that certifications be scalable and available to micro, small and medium-sized companies.<sup>14</sup> Such companies make up a large portion of the data ecosystem.

As mentioned, the ability to obtain GDPR certifications will be of significant value to organisations of all sizes. In addition to serving as both a general compliance tool and a cross-border transfer mechanism, certification will be particularly relevant to organisations choosing a trusted, certified data processor. Under Article 28.5 of the GDPR, the certification of a data processor can be used as “an element by which to demonstrate sufficient guarantees” of GDPR compliance, i.e. as a “due diligence” tool for controllers. Thus, certification will provide a significant benefit both to controllers seeking to retain processor services and to processors trying to demonstrate their accountability and differentiate themselves through certification from the rest of the market. But for this benefit to become broadly attainable, certifications must be widely available and affordable.

---

<sup>12</sup> See Footnote 1, at page 4 (Emphasis added).

<sup>13</sup> See Footnote 1, at page 5.

<sup>14</sup> Article 42(1) provides that “[t]he Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account”. (Emphasis added)

While certainly valuable and beneficial within their sphere of competency, ISO standards do not have a known track record of broad applicability for SMEs. The relevant data protection stakeholders, most notably the SAs and EDPB, should, therefore, devise a scalable accreditation and certification system that is suitable for the data protection context. Overly restrictive and cost-prohibitive accreditation standards will limit the range of available certification bodies in the ecosystem and will act as a barrier to entry for many certification bodies, as further discussed below. The lack of accredited certification bodies may lead to less choice and higher cost and, ultimately, may limit the number of certified organisations. Thus, together with the appropriate rigour, scalability and affordability must be priority considerations when developing accreditation criteria for certification bodies.

#### **IV. Accreditations by the National Accreditation Bodies and the Supervisory Authority**

It is critical to the successful uptake of GDPR certifications that a wide range of certification bodies can become accredited. Article 43.1, in fact, enables this by not limiting such accreditations to NABs but by also allowing SAs (and the EDPB) to develop separate accreditation requirements that can be specifically designed to address the scalability mandate in Article 42.1.

This additional route towards accreditation is particularly important as Regulation (EC) No. 765/2008 limits the number of NABs to one per Member State. This limitation, coupled with a potentially narrow accreditation standard (see discussion below), would result in limited numbers of certification bodies and certified companies.

Moreover, it remains to be seen whether the product-based scheme under Regulation (EC) No. 765/2008 will be effective in the novel context of an Article 42 certification applicable to a broad range of data processing operations. Thus, in order to maximise the range of organisations that are able to be certified (and in consideration of issues of scalability that are especially important to micro, small and medium-sized enterprises), it makes sense for the GDPR to allow SAs to develop accreditation standards based on EDPB-developed guidance and a model or template designed by the EDPB specifically for the specialised context of Article 42 privacy certifications with selective reference to ISO 17065 where appropriate. Such a model or template baseline accreditation standard developed by the EDPB would ensure consistency and mutual recognition between the accreditations by the SAs as well as maintain an appropriate level of consistency with the accreditation standards applicable to the NABs, as further discussed below. Requirements that may potentially be adopted by the Commission in accordance with Article 43.8 could also add value on this point. Moreover, to the extent such a standard can be developed taking into account the recognition criteria for certification bodies of other systems (such as the APEC CBPR and PRP), it would enable global interoperability and consistency as well. See discussion in Section VI below.

Indeed, the WP notes the absence of specific instructions in the GDPR on the criteria SAs must include in their accreditation requirements (other than the ones set forth in Article 43.2). This is in contrast to the more specific instructions pertaining to the accreditation criteria to be applied by the NABs. The fact that the GDPR does not set forth the same criteria for SA and NAP accreditation suggests the drafters' intent that the standards not be identical—as well as more flexibility granted to the SAs in exercise of their independent authority. However, the WP nevertheless concludes that “in the interest of contributing to a harmonized approach to accreditation” between the supervisory authorities and the national accreditation bodies, “the accreditation criteria used by the supervisory authority should be guided by ISO 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43.1(b)”.<sup>15</sup>

CIPL agrees that consistency is essential to providing a trusted certification ecosystem that enables mutual recognition of the accreditation criteria for certification bodies and of the certifications the system ultimately produces. Thus, consistency between the accreditation criteria for the NABs and the SAs is a legitimate and desirable goal, but it does not require that the standards be identical. Under the GDPR, consistency cannot be at the expense of scalability and accessibility of the certifications to organisations of all sizes. It must and can be achieved by creating “functional consistency” that aligns the key elements of the relevant accreditation standards rather than focuses on wholesale adoption of one standard (the ISO standard) that may be appropriate and workable for large organisations.

Indeed, the WP's phrase “should be guided by” correctly describes the relevance of the ISO standard for the accreditation criteria to be developed by the SAs (subject to and in line with EU-wide criteria developed by the EDPB). CIPL is simply flagging the importance of properly interpreting and applying the WP's “should be guided by” characterisation. As stated, and also as further discussed below, strict adherence to the ISO standard may lead to the introduction of prohibitive burdens and costs, thereby limiting the pool of potential certification bodies entering the market. A costly accreditation process or unsustainably high liabilities of certification bodies would create a more costly certification process for controllers and processors. This may practically render Article 42 certifications unavailable to micro, small and medium-sized organisations. Thus, the meaning of the WP's above phrasing of “should be guided by ISO 17065” should be clarified in the final Guidelines as leaving room for the necessary flexibility.

---

<sup>15</sup> See Footnote 1, at page 10 (Emphasis added). The WP also points out that the accreditation criteria in Article 43.2(a)-(e) already reflect and specify requirements of ISO 17065, noting that this will also contribute to consistency.

## V. ISO 17065

ISO 17065 sets forth standards for “Conformity assessment – Requirements for bodies certifying products, processes and services”, which are provided in eight sections and numerous subsections.<sup>16</sup> While under the GDPR the national accreditation bodies must accredit certification bodies “in accordance” with ISO 17065, the Draft Guidelines suggest that the SAs should also “be guided” by that standard. However, due to the nature of the ISO 17065 standard, a strict application of that standard could result in limited numbers of certification bodies and, ultimately, few certified organisations. The examples below demonstrate why that is the case. Thus, CIPL recommends the development of stand-alone GDPR-specific certification standards by the SAs (or the EDPB) with only selective reference to additional ISO standards where appropriate. To the extent the SAs (or the EDPB) look to the ISO standards in their own accreditation standards developed pursuant to Articles 43.1 and 43.3, the selection and phrasing should be done with an eye to enabling scalability and sufficient flexibility so that smaller certification bodies can be accredited.

Several examples from ISO 17065 cited below illustrate the potential negative effects of adopting the ISO standard in its entirety and/or without appropriate clarification and interpretation.

### Example 1: Section 4.3 on “Liability and Financing”

Section 4.3.1 provides that “[t]he certification body shall have adequate arrangements (e.g. insurance or reserves) to cover liabilities from its operations”.

This provision will have the effect of excluding potential certification bodies from being accredited, depending on how it is interpreted. As to the ability to “cover liabilities from its operations”, for this section to be workable in the GDPR certifications context, it should be interpreted to apply to a certification body’s ability to cover its general commercial liabilities. Liability should not be interpreted to include potential administrative fines for violations of the GDPR itself. This inclusion would effectively prohibit all but the very largest entities from serving as a certification body and functionally preclude most entities operating under a non-profit corporate structure. At the very least, the Working Party should clarify this in its guidelines.<sup>17</sup>

It is also unclear how this requirement would apply to SAs that choose to act as certification bodies, which indicates that the ISO standard, by definition, cannot be applied comprehensively to certifications provided by supervisory authorities.

---

<sup>16</sup> As mentioned and noted by the WP, Article 43.2—which applies to accreditations both by national accreditation bodies and SAs—already incorporates some elements of ISO 17065.

<sup>17</sup> In addition to the point that only general commercial liability should be covered under Section 4.3, certification bodies should only be liable for their own violations and not those of the organisations they certified. A good example might be the model followed by accounting firms, which do not accept liability for any misrepresentations in the financial statements of their clients.



There is some relevant international experience on privacy certifications in the context of conformity assessment. A notable case is Mexico, where Binding Self-Regulation parameters based on Mexican law equivalents of ISO 17065 were issued by the Mexican Data Protection Authority in 2014. These include similar requirements for certification and standardisation bodies. The result of the incorporation of ISO 17065 has been a very limited uptake by industry. To date only one certification and one standardisation body have been accredited.<sup>18</sup> Indeed, the anecdotal evidence from the Mexican experience suggests that the need to comply with overly prescriptive conformity assessment and normalisation requirements will exclude many organisations from becoming certifiers. That in turn concentrates the certification in a single authority and may increase the cost to the companies that seek certification.

**Example 2: Section 6.2 on “Resources for Evaluation”**

Section 6.2.1 provides that

“[w]hen a certification body performs evaluation activities, either with its internal resources or with other resources under its direct control, it shall meet the applicable requirements of the relevant International Standards and, as specified by the certification scheme, of other documents. For testing, it shall meet the applicable requirements of ISO/IEC 17025; for inspection, it shall meet the applicable requirements of ISO/IEC 17020; and for management system auditing, it shall meet the applicable requirements of ISO/IEC 17021. The impartiality requirements of the evaluation personnel stipulated in the relevant standard shall always be applicable”.

Strict adherence to ISO 17065 would necessarily require the introduction of additional ISO standards which may have limited utility in the performance of a GDPR-based privacy certification (e.g. ISO 17025 is designed to apply to the testing and/or calibration activities of laboratories). Further, the prescriptive application of requirements that are not specifically designed to address the unique nature of a GDPR-based privacy certification complicates the accreditation process and ultimately undermines the scalability goals of the GDPR and the harmonisation the WP guidance intends to foster.

**Example 3: Sections 7.4 - 7.6 “Review, Evaluation and Certification Decision”**

Section 7.4.2 provides that “[t]he certification body shall assign personnel to perform each evaluation task that it undertakes with its internal resources (see 6.2.1)”.

Section 7.5.1 further provides that “[t]he certification body shall assign at least one person to review all information and results related to the evaluation. The review shall be carried out by person(s) who have not been involved in the evaluation process”.

---

<sup>18</sup> More information can be found here: [http://rea.inai.org.mx/catalogs/masterpage/Sec6\\_1.aspx](http://rea.inai.org.mx/catalogs/masterpage/Sec6_1.aspx).



Finally Section 7.6.2 provides that “[t]he certification body shall assign at least one person to make the certification decision based on all information related to the evaluation, its review, and any other relevant information. The certification decision shall be carried out by a person or group of persons [e.g. a committee (see 5.1.4)] that has not been involved in the process for evaluation (see 7.4)”.

Taken together, Sections 7.4 - 7.6 introduce a multiple-step certification process that would, in effect, increase both the time and the costs associated with an Article 42 certification. We suggest that quality control can be effectively achieved through the development of the additional privacy-specific accreditation criteria contemplated by Article 43.2 (i.e. independence, subject matter expertise, having approved certification criteria and procedures, and an absence of a conflict of interest). Further, reliance on one set of criteria developed specifically for an Article 42 certification (though “guided by” the ISO standard where appropriate) would promote procedural harmonisation for accreditations by SAs, as well as sufficient consistency between SAs and NABs.

#### **Example 4: Section 7.9 on “Surveillance”**

Section 7.9.4 provides that

“[w]hen continuing use of a certification mark is authorized for a process or service, surveillance shall be established and shall include periodic surveillance activities to ensure ongoing validity of the demonstration of fulfilment of process or service requirements”.

Here it is critical that the concept of “surveillance” be given a reasonable and pragmatic interpretation that grants certification bodies sufficient discretion and flexibility to determine the appropriate level of ongoing monitoring, as well as the appropriate tools. Without such discretion and flexibility, this standard could easily result in unnecessary and disproportionate monitoring activities that will make providing certification services cost prohibitive to potential smaller certification bodies as well as to their customers. Again, this is an example of a criterion that must be applied in light of the GDPR mandate to make certifications accessible and scalable. Article 43.2(c) of the GDPR requires certification bodies to have “established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks” (Emphasis added). Periodic review does not equal surveillance. Surveillance implies a more structured and deeper requirement than a periodic review (which encompasses “spot checking”) and suggests a continuous process. Thus, to avoid the potentially debilitating impacts of such a process on the scalability of a GDPR certification system, there clearly is a need to apply Article 43.2(c) (“periodic review”) instead of the requirement in ISO 17065 Section 7.9.4.

## VI. ISO 17065 and the APEC Accountability Agent Recognition Criteria

In the APEC Cross-Border Privacy Rules (CBPR) and APEC Privacy Recognition for Processors (PRP) systems, certification bodies are called “Accountability Agents” (AAs). APEC has developed a comprehensive set of formal recognition criteria that APEC AAs must meet.<sup>19</sup> The APEC AA recognition criteria represent a rigorous yet flexible and scalable set of standards for AAs that could be instructive to both EU SAs and the EDPB in any process of developing an EU-wide accreditation standard for certification bodies certified by SAs. Importantly, there is substantial overlap and parity with respect to the essential accreditation or recognition criteria in both systems. In some cases, such as for example in connection with ISO 17065 Section 7.9.4 (regarding “surveillance”), the APEC correlate may be a useful example of how the same concept can be expressed in a way that reflects the necessary flexibility (i.e. “surveillance” (ISO) vs. “monitoring” and “review” upon notice of a possible violation (APEC)) .

As we noted in CIPL’s earlier discussion paper on GDPR certifications,<sup>20</sup> to facilitate EU-wide harmonisation and global interoperability, there should be a preference for one EU baseline certification for all contexts and sectors, with possible differentiation in its application, i.e. a “common certification” or “European Data Protection Seal” under Article 42.5 of the GDPR, developed under the lead of the Commission or the EDPB in collaboration with certification bodies and industry.<sup>21</sup> Similarly, there should be a common baseline accreditation standard approved by the EDPB under Article 64 (or the Commission under Article 43.8) for certification bodies accredited by the SAs. As discussed above, this baseline standard would ensure appropriate and functional intra-EU consistency across the various SAs that will be accrediting certification bodies under Article 43.1(a) and between the SAs and the NABs, as well as enable global consistency and interoperability with other systems.

Indeed, the Draft Guidelines note that “Member States and supervisory authorities should keep in mind the harmonised European level when formulating national law and procedures relating to accreditation and certification in accordance with the GDPR”.<sup>22</sup> Ultimately, such a common EU-wide approach to accreditation of certifications bodies that is developed with scalability and flexibility in mind will not only enable the express

---

<sup>19</sup> Accountability Agent – APEC Recognition Application (includes the recognition criteria), attached as Annex 1 hereto, available also at <https://cbprs.blob.core.windows.net/files/Accountability%20Agent%20Application%20for%20CBPR%20Revised%20For%20Posting%203-16.pdf>. See also the APEC recognition criteria for the PRP, which are identical as for the CBPR. They are available at <https://www.apec.org/~media/Files/Groups/ECSG/2015/Accountability%20Agent%20Application%20for%20the%20PRP%20System.pdf>.

<sup>20</sup> See Footnote 5.

<sup>21</sup> Thus, there may be many certification schemes in the EU, but they would be pegged to the same EU-wide baseline GDPR standard and would differ only in their context- or industry-specific adaptations. See CIPL’s white paper on certifications for details.

<sup>22</sup> See Footnote 1, at page 11.

goals of the GDPR but also the EU Commission's stated policy of promoting convergence or interoperability with non-EU cross-border transfer standards and systems, such as the APEC CBPR.<sup>23</sup>

### **Conclusion**

CIPL is grateful for the opportunity to provide comments on key implementation questions regarding the accreditation standards for certification bodies. We look forward to providing further input as the relevant accreditation standards are being developed, as well as to contributing generally to the development of effective and scalable GDPR certifications.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, [bbellamy@hunton.com](mailto:bbellamy@hunton.com); Markus Heyder, [mheyder@hunton.com](mailto:mheyder@hunton.com); or Sam Grogan, [sgrogan@hunton.com](mailto:sgrogan@hunton.com).

---

<sup>23</sup> See CIPL's discussion paper on certifications under the GDPR, Footnote 5 supra, discussing the 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](http://ec.europa.eu/newsroom/document.cfm?doc_id=41157).

# ANNEX



## ACCOUNTABILITY AGENT APEC RECOGNITION APPLICATION

<i>Overview .....</i>	<i>2</i>
<i>Application Process .....</i>	<i>2</i>
<i>ANNEX A: Accountability Agent Recognition Criteria .....</i>	<i>3</i>
<i>ANNEX B: Accountability Agent Recognition Criteria Checklist .....</i>	<i>10</i>
<i>ANNEX C: APEC CBPR Program Requirements Map .....</i>	<i>12</i>
<i>ANNEX D: Accountability Agent Case Notes/Template/FAQs .....</i>	<i>50</i>
<i>ANNEX E: Accountability Agent Complaint Statistics/Template/FAQs .....</i>	<i>56</i>
<i>ANNEX F: Signature and Contact Information .....</i>	<i>61</i>

## OVERVIEW

*The purpose of this document is to guide the application process for Accountability Agents seeking APEC recognition under the APEC Cross Border Privacy Rules (CBPR) System. This document explains the necessary recognition criteria and provides the baseline program requirements of the CBPR System. Only APEC-recognized Accountability Agents may participate in the CBPR System. Once recognized, Accountability Agents may publicize this recognition and certify organizations as CBPR compliant. A recognized Accountability Agent would only be able to certify as CBPR compliant those organizations that are subject to the enforcement authority of CPEA-participating privacy enforcement authorities within the economies in which it has been approved to operate.*

## APPLICATION PROCESS

In order to be considered eligible for recognition by APEC Economies, an Applicant Accountability Agent must:

- Explain how it is subject to the jurisdiction of the relevant enforcement authority in a CBPR participating Economy<sup>1</sup>; *AND*
- Describe how each of the Accountability Agent Recognition Criteria (Annex A) have been met using the Accountability Agent Recognition Criteria Checklist (Annex B); *AND*
- Agree to make use of the template documentation developed and endorsed by APEC Economies (the CBPR Intake Questionnaire<sup>2</sup> and the CBPR Program Requirements<sup>3</sup>) to assess applicant organizations when certifying organizations as CBPR-compliant; *OR* demonstrate how their existing intake and review processes meet the baseline established using the CBPR Program Requirements Map (Annex C<sup>4</sup>) and publish their program requirements; *AND*
- Complete the signature and contact information sheet (Annex F).

The completed signature and contact information sheet and all necessary supporting documentation should be submitted to the relevant government agencies or public authorities in any Economy in which the Applicant Accountability Agent intends to operate for an initial review to ensure the necessary documentation is included in the application, or other review as appropriate. The agency or authority may consult with other government agencies or authorities where necessary and will forward all information received to the Chair of the Electronic Commerce Steering Group, the Chair of the Data Privacy Subgroup and the Chair of the Joint Oversight Panel (JOP) where appropriate. The JOP will review the submitted information (and request any additional information that may be needed) when considering recommending the Applicant Accountability Agent for recognition by APEC Economies as an APEC CBPR System Accountability Agent.

---

<sup>1</sup> An Economy is considered a participant in the Cross Border Privacy Rules System pursuant to the terms established in Paragraph 2.2 of the "Charter of the APEC Cross-Border Privacy Rules System Joint Oversight Panel" (*available at [http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11\\_ecsg2\\_012.pdf](http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11_ecsg2_012.pdf)*)

<sup>2</sup> Available at [http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11\\_ecsg2\\_014.doc](http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11_ecsg2_014.doc)

<sup>3</sup> Available at [http://aimp.apec.org/Documents/2011/ECSG/DPS2/11\\_ecsg\\_dps2\\_007.doc](http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_007.doc)

<sup>4</sup> Annex C should be read consistently with the APEC Cross Border Privacy Rules Intake Questionnaire which lists the acceptable qualifications to the provision of notice, the provision of choice mechanisms, and the provision of access and correction mechanisms referred to in this document.

## ACCOUNTABILITY AGENT RECOGNITION CRITERIA

### CRITERIA

#### *Conflicts of Interest*

1) General Requirements:

- a. An Accountability Agent must be free of actual or potential conflicts of interest in order to participate in the APEC Cross Border Privacy Rules (CBPR) System. For the purposes of participation as an Accountability Agent in the CBPR System, this means the ability of the Accountability Agent to perform all tasks related to an Applicant organization's certification and ongoing participation in the CBPR System free from influences that would compromise the Accountability Agent's professional judgment, objectivity and integrity.
- b. An Accountability Agent must satisfy the APEC member economies with evidence that internal structural and procedural safeguards are in place to address potential and actual conflicts of interest. Such safeguards should include but not be limited to:
  - i. Written policies for disclosure of potential conflicts of interest and, where appropriate, withdrawal of the Accountability Agent from particular engagements. Such withdrawal will be required in cases where the Accountability Agent is related to the Applicant organization or Participant to the extent that it would give rise to a risk that the Accountability Agent's professional judgment, integrity, or objectivity could be influenced by the relationship.
  - ii. Written policies governing the separation of personnel handling privacy certification functions from personnel handling sales and consulting functions.
  - iii. Written policies for internal review of potential conflicts of interest with Applicant organizations and Participating organizations.
  - iv. Published certification standards for Applicant organizations and Participating organizations (see paragraph 4 'Program Requirements').
  - v. Mechanisms for regular reporting to the relevant government agency or public authority on certification of new Applicant organizations, audits of existing Participant organizations, and dispute resolution.
  - vi. Mechanisms for mandatory publication of case reports in certain circumstances.

2) Requirements with respect to particular Applicant organizations and/or Participant organizations

- a. At no time may an Accountability Agent have a direct or indirect affiliation with any Applicant organization or Participant organization that would prejudice the ability of the Accountability agent to render a fair decision with respect to their certification and ongoing participation in the CBPR System, including but not limited to during the application review and initial certification process; during ongoing monitoring and compliance review; during re-certification and annual attestation; and during dispute resolution and enforcement of the Program Requirements against a Participant. Such affiliations, which include but are not limited to the Applicant organization or Participant organization and the Accountability Agent being under common control such that the Applicant organization or Participant organization can exert undue influence in the Accountability Agent, constitute relationships that require withdrawal under 1(b)(i).
- b. For other types of affiliations that may be cured by the existence of structural safeguards or other procedures undertaken by the Accountability Agent, the existence of any such affiliations between the Accountability Agent and the Applicant organization or Participant organization must be disclosed promptly to the Joint Oversight Panel, together with an explanation of the safeguards in place to ensure that such affiliations do not compromise the Accountability Agent's ability to render a fair decision with respect to such an Applicant organization or Participant organization. Such affiliations include but are not limited to:
  - i. officers of the Applicant organization or Participant organization serving on the Accountability Agent's board of directors in a voting capacity, and vice versa;
  - ii. significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant organization or Participant organization, outside of the fee charged for certification and participation in the APEC CBPR System; or
  - iii. all other affiliations which might allow the Applicant organization or Participant organization to exert undue influence on the Accountability Agent regarding the Applicant organization's certification and participation in the CBPR System.
- c. Outside of the functions described in paragraphs 5-14 of this document, an Accountability Agent will refrain from performing for its Participants or Applicants services for a fee or any interest or benefit such as the following categories:
  - i. consulting or technical services related to the development or implementation of Participant organization's or Applicant organization's data privacy practices and procedures;
  - ii. consulting or technical services related to the development of its privacy policy or statement; or



- iii. consulting or technical services related to its security safeguards.
  - d. An Accountability Agent may be engaged to perform consulting or technical services for an Applicant organization or Participant organization other than services relating to their certification and on-going participation in the CBPR System. Where this occurs, the Accountability Agent will disclose to the Joint Oversight Panel:
    - i. the existence of the engagement; and
    - ii. an explanation of the safeguards in place to ensure that the Accountability Agent remains free of actual or potential conflicts of interest arising from the engagement [*such safeguards may include segregating the personnel providing the consulting or technical services from the personnel performing the functions described in paragraphs 5 -14 of this document*].
  - e. Provision of services as required in Sections 3 through 6 shall not be considered performing consulting services which might trigger a prohibition contained in this document.
- 3) In addition to disclosing to the Joint Oversight Panel all withdrawals described above in Section 1(b)(i), an Accountability Agent also shall disclose to the Joint Oversight Panel those activities or business ventures identified in subsection 1(b) above that might on their face have been considered a conflict of interest but did not result in withdrawal. Such disclosures should include a description of the reasons for non-withdrawal and the measures the Accountability Agent took to avoid or cure any potential prejudicial results stemming from the actual or potential conflict of interest.

### ***Program Requirements***

- 4) An Accountability Agent evaluates Applicant organizations against a set of program requirements that encompass all of the principles of the APEC Privacy Framework with respect to cross border data transfers and that meet the CBPR program requirements developed and endorsed by APEC member economies (to be submitted along with this form, see Annex A). (*NOTE: an Accountability Agent may charge a fee to a Participant for provision of these services without triggering the prohibitions contained in paragraph 1 or 2.*)

### ***Certification Process***

- 5) An Accountability Agent has a comprehensive process to review an Applicant organization's policies and practices with respect to the Applicant organization's participation in the Cross Border Privacy Rules System and to verify its compliance with the Accountability Agent's program requirements. The certification process includes:
  - a) An initial assessment of compliance, which will include verifying the contents of the self-assessment forms completed by the Applicant organization against the program requirements for Accountability Agents, and which may also

include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.

- b) A comprehensive report to the Applicant organization outlining the Accountability Agent's findings regarding the Applicant organization's level of compliance with the program requirements. Where non-fulfillment of any of the program requirements is found, the report must include a list of changes the Applicant organization needs to complete for purposes of obtaining certification for participation in the CBPR System.
- c) Verification that any changes required under subsection (b) have been properly completed by the Applicant organization.
- d) Certification that the Applicant organization is in compliance with the Accountability Agent's program requirements. An Applicant organization that has received such a certification will be referred to herein as a "Participant" in the CBPR System.
- e) Provision of the relevant details of the Participant's certification for the Compliance Directory.<sup>1</sup> The relevant details should include at least the following: the name of the certified organization, a website for the certified organization and a link to the organization's privacy policy, contact information, the Accountability Agent that certified the Participant and can handle consumer disputes, the relevant Privacy Enforcement Authority, the scope of the certification, the organization's original certification date, and the date that the current certification expires.

### ***On-going Monitoring and Compliance Review Processes***

- 6) Accountability Agent has comprehensive written procedures designed to ensure the integrity of the Certification process and to monitor the Participant throughout the certification period to ensure compliance with the Accountability Agent's program.
- 7) In addition, where there are reasonable grounds for the Accountability Agent to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate review process will be triggered whereby verification of compliance will be carried out. Where non-compliance with any of the program requirements is found, the Accountability Agent will notify the Participant outlining the corrections the Participant needs to make and a reasonable timeframe within which the corrections must be completed. The Accountability Agent must verify that the required changes have been properly completed by the Participant within the stated timeframe.

### ***Re-Certification and Annual Attestation***

- 8) Accountability Agent will require Participants to attest on an annual basis to the continuing adherence to the CBPR program requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-Certification. Where there has been a material change to the Participant's privacy policy (as reasonably determined by the Accountability Agent in good faith), an

---

<sup>1</sup> See "APEC Cross Border Privacy Rules System Policies, Rules and Guidelines," paragraph 14 (*available at* [http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11\\_ecsg2\\_012.pdf](http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11_ecsg2_012.pdf)).

immediate review process will be carried out. This re-certification review process includes:

- a) An assessment of compliance, which will include verification of the contents of the self-assessment forms (Project 1) updated by the Participant, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.
- b) A report to the Participant outlining the Accountability Agent's findings regarding the Participant's level of compliance with the program requirements. The report must also list any corrections the Participant needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification.
- c) Verification that required changes have been properly completed by Participant.
- d) Notice to the Participant that the Participant is in compliance with the Accountability Agent's program requirements and has been re-certified.

### ***Dispute Resolution Process***

- 9) An Accountability Agent must have a mechanism to receive and investigate complaints about Participants and to resolve disputes between complainants and Participants in relation to non-compliance with its program requirements, as well as a mechanism for cooperation on dispute resolution with other Accountability Agents recognized by APEC economies when appropriate and where possible. Such mechanism must be publicized on the Participant's website. An Accountability Agent may choose not to directly supply the dispute resolution mechanism. The dispute resolution mechanism may be contracted out by an Accountability Agent to a third party for supply of the dispute resolution service. Where the dispute resolution mechanism is contracted out by an Accountability Agent the relationship must be in place at the time the Accountability Agent is certified under the APEC CBPR system. An Accountability Agent's website must include the contact point information for the relevant Privacy Enforcement Authority. Publicizing such contact point information allows consumers or other interested parties to direct questions and complaints to the relevant Accountability Agent, or if necessary, to contact the relevant Privacy Enforcement Authority.
- 10) The dispute resolution process, whether supplied directly or by a third party under contract, includes the following elements:
  - a) A process for receiving complaints and determining whether a complaint concerns the Participant's obligations under the program and that the filed complaint falls within the scope of the program's requirements.
  - b) A process for notifying the complainant of the determination made under subpart (a), above.
  - c) A process for investigating complaints.
  - d) A confidential and timely process for resolving complaints. Where non-

compliance with any of the program requirements is found, the Accountability Agent or contracted third party supplier of the dispute resolution service will notify the Participant outlining the corrections the Participant needs to make and the reasonable timeframe within which the corrections must be completed.

- e) Written notice of complaint resolution by the Accountability Agent or contracted third party supplier of the dispute resolution service to the complainant and the Participant.
- f) A process for obtaining an individual's consent before sharing that individual's personal information with the relevant enforcement authority in connection with a request for assistance.
- g) A process for making publicly available statistics on the types of complaints received by the Accountability Agent or contracted third party supplier of the dispute resolution service and the outcomes of such complaints, and for communicating that information to the relevant government agency and privacy enforcement authority (see Annex E).
- h) A process for releasing in anonymised form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes (see Annex D).

### ***Mechanism for Enforcing Program Requirements***

- 11) Accountability Agent has the authority to enforce its program requirements against Participants, either through contract or by law.
- 12) Accountability Agent has a process in place for notifying Participant immediately of non-compliance with Accountability Agent's program requirements and for requiring Participant to remedy the non-compliance within a specified time period.
- 13) Accountability Agent has processes in place to impose the following penalties, which is proportional to the harm or potential harm resulting from the violation, in cases where a Participant has not complied with the program requirements and has failed to remedy the non-compliance within a specified time period. [NOTE: In addition to the penalties listed below, Accountability Agent may execute contracts related to legal rights and, where applicable, those related intellectual property rights enforceable in a court of law.]
  - a) Requiring Participant to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall remove the Participant from its program.
  - b) Temporarily suspending the Participant's right to display the Accountability Agent's seal.
  - c) Naming the Participant and publicizing the non-compliance.
  - d) Referring the violation to the relevant public authority or privacy enforcement authority. [NOTE: this should be reserved for circumstances where a violation raises to the level of a violation of applicable law.]

e) Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent.

14) Accountability Agent will refer a matter to the appropriate public authority or enforcement agency for review and possible law enforcement action, where the Accountability Agent has a reasonable belief pursuant to its established review process that a Participant's failure to comply with the APEC Cross-Border Privacy Rules System requirements has not been remedied within a reasonable time under the procedures established by the Accountability Agent pursuant to paragraph 2 so long as such failure to comply can be reasonably believed to be a violation of applicable law.

15) Where possible, Accountability Agent will respond to requests from enforcement entities in APEC Economies that reasonably relate to that Economy and to the CBPR- related activities of the Accountability Agent.

## **ACCOUNTABILITY AGENT RECOGNITION CRITERIA CHECKLIST**

### **Conflicts of Interest**

1. Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.
2. Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A.
3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

### **Program Requirements**

4. Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.

### **Certification Process**

5. Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d) of Annex A have been met.

### **On-going Monitoring and Compliance Review Processes**

6. Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d).
7. Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.

### **Re-Certification and Annual Attestation**

8. Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d) of Annex A.

### **Dispute Resolution Process**

9. Applicant Accountability Agent should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents that may be used when appropriate.
10. Applicant Accountability Agent should describe how the dispute resolution process meets the requirements identified in 10 (a) – (h) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third

party supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E.

### **Mechanism for Enforcing Program Requirements**

11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.
12. Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance.
13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.
14. Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].
15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

**APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM  
REQUIREMENTS MAP**

NOTICE.....	13
COLLECTION LIMITATION.....	19
USES OF PERSONAL INFORMNATION .....	21
CHOICE.....	25
INTEGRITY OF PERSONAL INFORMATION .....	31
SECURITY SAFEGUARDS .....	34
ACCESS AND CORRECTION .....	40
ACCOUNTABILITY .....	44
GENERAL .....	44
MAINTAINING ACCOUNTABILITY WHEN PERSONAL INFORMATION IS TRANSFERRED .....	47



## NOTICE

**Assessment Purpose** – *To ensure that individuals understand the applicant organization's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	<p>If <b>YES</b>, the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics:</p> <ul style="list-style-type: none"><li>• Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified).</li><li>• Is in accordance with the principles of the APEC Privacy Framework;</li><li>• Is easy to find and accessible.</li><li>• Applies to all personal information; whether collected online or offline.</li><li>• States an effective date of Privacy Statement publication.</li></ul> <p>Where Applicant answers <b>NO</b> to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies</p>	

	an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.a) Does this privacy statement describe how personal information is collected?	<p>If <b>YES</b>, the Accountability Agent must verify that:</p> <ul style="list-style-type: none"> <li>• The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant.</li> <li>• the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and</li> <li>• The Privacy Statement reports the categories or specific sources of all categories of personal information collected.</li> </ul> <p>If <b>NO</b>, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.</p>	
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	
1.c) Does this privacy	Where the Applicant answers <b>YES</b> , the	

statement inform individuals whether their personal information is made available to third parties and for what purpose?	<p>Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant provides name, address and a <b>functional</b> e-mail address.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	
1.e) Does this privacy statement provide information regarding the use and disclosure of an	Where the Applicant answers <b>YES</b> , the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all	

individual's personal information?	personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers <b>NO</b> and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Privacy Statement includes:</p> <ul style="list-style-type: none"> <li>• The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means).</li> <li>• The process that an individual must follow in order to correct his or her personal information</li> </ul> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	
2. Subject to the qualifications listed below,	Where the Applicant answers <b>YES</b> , the Accountability Agent must verify that the Applicant	

at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	<p>provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	
4. Subject to the	Where the Applicant answers <b>YES</b> , the	

<p>qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?</p>	<p>Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.</p>	
--	---	--

## COLLECTION LIMITATION

**Assessment Purpose** - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair*

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
<p>5. How do you obtain personal information:</p> <p>5.a) Directly from the individual?</p> <p>5.b) From third parties collecting on your behalf?</p> <p>5.c) Other. If YES, describe.</p>	<p>The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information.</p> <p>Where the Applicant answers <b>YES</b> to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard.</p> <p>There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.</p>	
<p>6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?</p>	<p>Where the Applicant answers <b>YES</b> and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify:</p> <ul style="list-style-type: none"> <li>• Each type of data collected</li> <li>• The corresponding stated purpose of collection for each; and</li> <li>• All uses that apply to each type of data</li> <li>• An explanation of the compatibility or relatedness of each identified use with the stated purpose of</li> </ul>	

	<p>collection</p> <p>Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.</p>	
<p>7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.</p>	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception.</p> <p>Where the Applicant Answers <b>NO</b>, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.</p>	



## USES OF PERSONAL INFORMATION

**Assessment Purpose** - Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant answers <b>YES</b> , the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes.  Where the Applicant Answers <b>NO</b> , the Accountability Agent must consider answers to Question 9 below.	
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following	Where the Applicant answers <b>NO</b> to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require	



parties acting on your behalf) to other personal information controllers? If YES, describe.	and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law.	
11. Do you transfer personal information to personal information processors? If YES, describe.	Also, the Accountability Agent must require the Applicant to identify:	
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.	<ol style="list-style-type: none"> <li>1) each type of data disclosed or transferred;</li> <li>2) the corresponding stated purpose of collection for each type of disclosed data; and</li> <li>3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.).</li> </ol> <p>Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.</p>	
<p>13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?</p> <p>13.a) Based on express consent of the individual?</p> <p>13.b) Necessary to provide a service or product requested by the individual?</p> <p>13.c) Compelled by</p>	<p>Where applicant answers <b>NO</b> to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes.</p> <p>Where the Applicant answers <b>YES</b> to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as:</p> <ul style="list-style-type: none"> <li>• Online at point of collection</li> <li>• Via e-mail</li> </ul>	

applicable laws?	<ul style="list-style-type: none"> <li>• Via preference/profile page</li> <li>• Via telephone</li> <li>• Via postal mail, or</li> <li>• Other (in case, specify)</li> </ul> <p>Where the Applicant answers <b>YES</b> to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual.</p> <p>Where the Applicant answers <b>YES</b> to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement.</p> <p>Where the Applicant answers <b>NO</b> to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.</p>	
------------------	---	--

## CHOICE

**Assessment Purpose** - Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as:</p> <ul style="list-style-type: none"><li>• Online at point of collection</li><li>• Via e-mail</li><li>• Via preference/profile page</li><li>• Via telephone</li><li>• Via postal mail, or</li><li>• Other (in case, specify)</li></ul> <p>The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated.</p> <p>Where the Applicant answers <b>NO</b>, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers <b>NO</b> and does not identify an applicable qualification the Accountability</p>	

	Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as:</p> <ul style="list-style-type: none"> <li>• Online at point of collection</li> <li>• Via e-mail</li> <li>• Via preference/profile page</li> <li>• Via telephone</li> <li>• Via postal mail, or</li> <li>• Other (in case, specify)</li> </ul> <p>The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:</p> <ul style="list-style-type: none"> <li>• being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and</li> <li>• Personal information may be disclosed or distributed to third parties, other than Service</li> </ul>	

	<p>Providers.</p> <p>Where the Applicant answers <b>NO</b>, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.</p>	
<p>16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.</p>	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as:</p> <ul style="list-style-type: none"> <li>• Online at point of collection</li> <li>• Via e-mail</li> <li>• Via preference/profile page</li> <li>• Via telephone</li> <li>• Via postal mail, or</li> <li>• Other (in case, specify)</li> </ul> <p>The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise</p>	

	<p>choice may be provided to the individual after collection, but before:</p> <ul style="list-style-type: none"> <li>disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.]</li> </ul> <p>Where the Applicant answers <b>NO</b>, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.</p>	
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner .</p> <p>Where the Applicant answers <b>NO</b>, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.</p>	
18. When choices are	Where the Applicant answers <b>YES</b> , the Accountability	



provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	<p>Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable.</p> <p>Where the Applicant answers <b>NO</b>, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.</p>	
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable.</p> <p>Where the Applicant answers <b>NO</b>, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.</p>	
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	<p>Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored.</p> <p>Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the</p>	

	<p>Accountability Agent must verify whether the applicable qualification is justified.</p> <p>Where the Applicant answers <b>NO</b> and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.</p>	
--	---	--

## INTEGRITY OF PERSONAL INFORMATION

**Assessment Purpose** - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use.</p> <p>The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.</p>	
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax,</p>	

attachment if necessary.	<p>through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.</p>	
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf.</p> <p>The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.</p>	
24. Where inaccurate, incomplete or out of date information will affect the	Where the Applicant answers <b>YES</b> , the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate	

<p>purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.</p>	<p>corrections to other third parties, to whom personal information was disclosed.</p> <p>The Accountability Agent must verify that these procedures are in place and operational.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.</p>	
<p>25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?</p>	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated.</p> <p>The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.</p>	

## SECURITY SAFEGUARDS

**Assessment Purpose** - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
26. Have you implemented an information security policy?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify the existence of this written policy.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.</p>	
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	<p>Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include:</p> <ul style="list-style-type: none"> <li>• Authentication and access control (eg password protections)</li> <li>• Encryption</li> <li>• Boundary protection (eg firewalls, intrusion detection)</li> <li>• Audit logging</li> <li>• Monitoring (eg external and internal audits, vulnerability scans)</li> <li>• Other (specify)</li> </ul> <p>The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's</p>	

	<p>size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.</p> <p>Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.</p> <p>The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.</p> <p>Where the Applicant indicates that it has <b>NO</b> physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.</p>	
<p>28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.</p>	<p>Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified.</p> <p>The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that</p>	

	information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	<p>The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include:</p> <ul style="list-style-type: none"> <li>• Training program for employees</li> <li>• Regular staff meetings or other communications</li> <li>• Security policy signed by employees</li> <li>• Other (specify)</li> </ul> <p>Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.</p>	
<p>30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:</p> <p>30.a) Employee training and management or other safeguards?</p> <p>30.b) Information systems and management, including</p>	<p>Where the Applicant answers <b>YES</b> (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards.</p> <p>The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information.</p> <p>Where the Applicant answers <b>NO</b> (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for</p>	



<p>network and software design, as well as information processing, storage, transmission, and disposal?</p> <p>30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?</p> <p>30.d) Physical security?</p>	<p>compliance with this principle.</p>	
<p>31. Have you implemented a policy for secure disposal of personal information?</p>	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.</p>	
<p>32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?</p>	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.</p>	
<p>33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe</p>	<p>The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.</p>	

below.		
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	
<p>35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:</p> <p>35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?</p> <p>35.b) Notifying you promptly when they become aware of an occurrence of breach of the</p>	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	

<p>privacy or security of the personal information of the Applicant's customers?</p> <p>35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?</p>		
---	--	--

## ACCESS AND CORRECTION

**Assessment Purpose** - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

*The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.*

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests.</p> <p>The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity.</p> <p>The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information.</p> <p>The personal information must be provided to individuals</p>	

	<p>in an easily comprehensible way.</p> <p>The Applicant must provide the individual with a time frame indicating when the requested access will be granted.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	
<p>37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38.</p> <p>37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.</p> <p>37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe.</p> <p>37.c) Is information</p>	<p>Where the Applicant answers <b>YES</b> the Accountability Agent must verify each answer provided.</p> <p>The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information.</p> <p>If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate.</p> <p>Where the Applicant answers <b>NO</b> and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	

<p>communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.</p> <p>37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?</p> <p>37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.</p>		
<p>38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e).</p> <p>38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.</p>	<p>Where the Applicant answers <b>YES to questions 38.a</b>, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy.</p> <p>If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate.</p> <p>All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting</p>	

<p>38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?</p> <p>38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?</p> <p>38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted?</p> <p>38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?</p>	<p>individual.</p> <p>Where the Applicant answers <b>NO</b> to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>	
--	---	--

## ACCOUNTABILITY

**Assessment Purpose** - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
<p>39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe.</p> <ul style="list-style-type: none"><li>• Internal guidelines or policies (if applicable, describe how implemented) _____</li><li>• Contracts _____</li><li>• Compliance with applicable industry or sector laws and regulations _____</li><li>• Compliance with self-regulatory applicant code and/or rules _____</li></ul>	<p>The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.</p>	



<ul style="list-style-type: none"> <li>• Other (describe) _____</li> </ul>		
<p>40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?</p>	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles.</p> <p>The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.</p>	
<p>41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.</p>	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as:</p> <ol style="list-style-type: none"> <li>1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR</li> <li>2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR</li> <li>3) A formal complaint-resolution process; AND/OR</li> </ol>	

	<p>4) Other (must specify).</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>	
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>	
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints.</p> <p>Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.</p>	
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure	Where the Applicant answers <b>YES</b> , the Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the	

of personal information?	necessary training to employees regarding this subject.  Where the Applicant answers <b>NO</b> , the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	
<p>46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?</p> <ul style="list-style-type: none"> <li>• Internal guidelines or policies _____</li> <li>• Contracts _____</li> <li>• Compliance with applicable industry or sector laws and regulations _____</li> <li>• Compliance with self-regulatory applicant code and/or rules _____</li> <li>• Other (describe) _____</li> </ul>	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify the existence of each type of agreement described.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.</p>	
<p>47. Do these agreements generally require that personal information processors, agents, contractors or other service providers:</p> <ul style="list-style-type: none"> <li>• Abide by your APEC-</li> </ul>	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	

<p>compliant privacy policies and practices as stated in your Privacy Statement? _____</p> <ul style="list-style-type: none"> <li>• Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____</li> <li>• Follow instructions provided by you relating to the manner in which your personal information must be handled? _____</li> <li>• Impose restrictions on subcontracting unless with your consent? _____</li> <li>• Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____</li> <li>• Notify the Applicant in the case of a breach of the personal information of the Applicant's customers?</li> <li>• Other (describe) _____</li> </ul>		
<p>48. Do you require your personal information processors, agents, contractors or other service providers to provide you</p>	<p>The Accountability Agent must verify the existence of such self-assessments.</p>	

with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.		
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.</p>	
50. Do you disclose personal information to other recipient <b><u>persons or organizations</u></b> in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	<p>If <b>YES</b>, the Accountability Agent must ask the Applicant to explain:</p> <p>(1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and</p> <p>(2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.</p>	

## **ACCOUNTABILITY AGENT CASE NOTES**

The Accountability Agent Recognition Criteria require applicants to attest that as part of their dispute resolution mechanism they have a process for releasing, in anonymised form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes.

The template, with associated guidance and FAQs, will assist in meeting the requirement.

### ***Objectives of Release of Case Notes***

Complaints handling is an important element of the Cross-border Privacy Rules (CBPR) program. The recognition criteria for Accountability Agents include an obligation to release case notes on a selection of resolved complaints in order to:

- promote understanding about the operation of the CBPR program;
- assist consumers and businesses and their advisers;
- facilitate consistency in the interpretation of the APEC information privacy principles and the common elements of the CBPR program;
- increase transparency in the CBPR program; and
- promote accountability of those involved in complaints handling and build stakeholder trust in accountability agents.

### ***Commentary on the Template***

The template is provided as a tool for Accountability Agents. It is acceptable to depart from the template for stylistic reasons by, for example, reordering the elements (e.g. by switching the date and citation to different ends of the note) or adding additional elements. However, it would be difficult to produce a satisfactory case note without the minimum elements mentioned in the template.

#### ***General heading***

It is possible to combine the general heading and citation into a single heading or adopt a citation that stands in for a general heading. However, unlike a series of law reports directed exclusively at lawyers, case notes are useful as an educational tool for ordinary consumers and businesses. Accordingly, a general heading that communicates a clear straightforward message is recommended.

#### ***Citation***

It is essential that all those that may wish to refer to a case note can do so by an accepted citation that unambiguously refers to the same note. All case notes should be issued with a citation including the following elements:

- a descriptor of the case;
- the year of publication ;

- a standard abbreviation for the accountability authority (including an indicator of which economy the Accountability Agent is based), and;
- a sequential number.

### *Case report*

The style and approach of case reports can differ substantially but there are several elements that almost certainly will appear. These include:

- an account of the facts (e.g. as initially asserted on a complaint and as found after investigation)
- the relevant law (which will include the elements of the CBPR program)
- a discussion of the issues of interest and how the law applied to the facts in question
- the outcome of the complaint.

### *Key terms*

It may be useful to include the standard terms used in traditional indexing or which will appear as tags in on-line environments.

## CASE NOTE TEMPLATE

General heading

Citation

Case report

- Facts
- Law
- Discussion
- Outcome

Date

Key terms

- Tags



## CASE NOTE FREQUENTLY ASKED QUESTIONS

*Q. How many case notes should an Accountability Agent publish?*

A. Those responsible for a CBPR program may find it useful to set targets for how many case notes should be published and make those targets public. In the initial years of a scheme's operation a greater number of case notes may be warranted so as to assist advisers and to provide reassurance to regulators and others. In later years, when there is a greater body of case notes available, fewer new notes may be needed. A scheme handling very few complaints will need to report a greater proportion of its complaints than a large scheme which can be more selective. As a general guide, a scheme handling more than 200 complaints a year might aim to publish about 8-10% of that number in case notes in the early years dropping later to, perhaps, 3-5 %.

*Q. Which resolved complaints should be selected for case notes?*

A. Those responsible for a CBPR program may find it useful to adopt standards to be applied in selecting case suitable for reporting. For instance, to ensure that the more serious cases are identified for reporting, criteria might refer to such indicators of systemic impact such as size of monetary settlements or awards. There is a need to report cases including significant or novel interpretations. There is also a value in reporting some typical cases which raise no novel legal issues but which illustrate the operation of the CBPR program in action.

*Q. Why are case notes typically reported in anonymous form?*

A. Case notes seek to illustrate the operation of the CBPR scheme, to educate about matters of interpretation and to ensure those handling complaints remain accountable. These objectives do not necessarily require the respondent to be named. The major objective of the complaints system is to resolve consumer disputes. Subject to the requirements of any particular scheme, this is often facilitated by confidential conciliation or mediation between the parties which does not require, and may even be hampered by, naming respondents publicly.

*Q. Might it be useful to name respondents sometimes?*

A. Sometimes it will be appropriate to name the respondent to a complaint. Indeed, some CBPR programs might have this as their usual practice. Even programs that do not usually name respondents may need to do so sometimes, for instance where the respondent has publicly announced that the program is handling the complaint or that fact has otherwise become a matter of public notoriety. Occasionally, naming a respondent is an intentional part of the complaint outcome (e.g. if the respondent is refusing to cooperate with the investigation or accept the outcome). It will be good practice for Accountability Agents to adopt transparent policies on their practices for naming respondents.

*Q. How much detail should appear in the case notes?*

A. When publishing case notes in anonymous form, care needs to be taken in publishing details which might inadvertently identify the parties. Anonymity is usually easily achieved through generalizing factual details. The level of useful detail in a particular case note will depend upon why it has been chosen for reporting. For example, complaints selected for a case note to illustrate a novel matter of legal interpretation will need the legal reasoning to be set out in full detail. By contrast, a case-note illustrating a fairly routine interpretation in an interesting factual-setting will obviously pay more attention to the facts. In the early phases of a scheme, relatively simple case notes are acceptable to ensure that advisers understand basic concepts but these should be followed by more detailed notes as familiarity with basic concepts is established.

*Q. How should Accountability Agents disseminate case notes?*

A. Active steps should be taken to make case notes easily available. Useful approaches may include to:

- maintain a distribution list to which copies of case notes are emailed
- release case notes individually or in batches during the year with accompanying media statements
- prepare summaries and use these in newsletters to highlight the release of new case notes
- post case notes on the Accountability Agent's website with good indexing and retrieval tools
- distribute electronic copies through RSS feeds
- integrate case notes into other educative initiatives such as training packages
- co-operate in re-publication by legal publishers.

*Q. How can Accountability Agents assist in making case notes readily available throughout the Asia Pacific?*

A. The cross-border nature of a CBPR program means that case notes will be useful to consumers, businesses, regulators and advisers in a variety of economies and not just in the Accountability Agent's home economy. Extra efforts should be taken to make their case notes widely available. These extra efforts will also contribute to consistency in interpretation across the region. Two key steps that Accountability Agents can take to make their case notes accessible throughout the Asia Pacific include:

- to facilitate the efforts of those who wish to re-publish their case notes
- to provide their case notes, in electronic form, to a recognised international consolidated point of access.

*Q. How can Accountability Agents facilitate the efforts of those who wish to republish their case notes?*

A. Third party publishers can enable case notes to be made more widely available to the public, specialist bodies, advisers, researchers and regulators. Accountability Agents may facilitate re-publication by giving a general license for re-publication of case notes with

proper acknowledgement. The general license should be included with the usual copyright statement posted on an Accountability Agent's website.

*Q. Is there a place where all case notes could be deposited and accessed?*

A. There is considerable value in having consolidated point of access for case notes from a variety of privacy enforcement authorities and accountability agents. The World Legal Information Institute's International Privacy Law Library available at [www.worldlii.org/int/special/privacy](http://www.worldlii.org/int/special/privacy) provides a specialist facility for hosting privacy case notes and has for many years published case notes from privacy enforcement authorities in various Asia Pacific economies. The consolidated access point brings a variety of benefits including the ability to search seamlessly across a range of case note series from within the region. Accountability Agents are encouraged to make arrangements with WorldLII for the supply of case notes and their republication.

*Q. Is there any further published guidance on releasing case notes?*

A. The following resources discuss issues in releasing case notes and provide examples:

- International Privacy Law Library available at [www.worldlii.org/int/special/privacy](http://www.worldlii.org/int/special/privacy) - which includes many examples of privacy case note series
- Graham Greenleaf, 'Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability for Asia-Pacific Privacy Commissioners', 2004 available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=512782](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=512782)
- Asia-Pacific Privacy Authorities Statement of Common Administrative Practice on Case Note Citation, November 2005, available at [www.privacy.gov.au/international/appa/statement.pdf](http://www.privacy.gov.au/international/appa/statement.pdf)
- Asia-Pacific Privacy Authorities Statement of Common Administrative Practice on Case Note Dissemination, November 2006, available at [www.privacy.gov.au/international/appa/statement2.pdf](http://www.privacy.gov.au/international/appa/statement2.pdf)
- OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, 2007, clause 20, available at [www.oecd.org/dataoecd/43/28/38770483.pdf](http://www.oecd.org/dataoecd/43/28/38770483.pdf)

## **ACCOUNTABILITY AGENT COMPLAINT STATISTICS**

The Accountability Agent recognition criteria require applicant Accountability Agents to attest that as part of their dispute resolution mechanism they have a process for releasing complaint statistics and for communicating that information to the relevant government agency and privacy enforcement authority.

The template, with associated guidance and FAQs will assist in meeting the requirement.

### ***Objectives of Reporting Complaint Statistics***

Complaints handling is an important element of the Cross-Border Privacy Rules (CBPR) program. The recognition criteria for Accountability Agents include an obligation to publish and report statistics on complaints received in order to:

- promote understanding about the operation of the CBPR program;
- increase transparency across the CBPR system;
- help governments, business and others to see how a complaints system is working and to help identify trends;
- enable comparisons of parts of the CBPR program across the APEC region; and
- promote accountability of those involved in complaints handling and build stakeholder trust in Accountability Agents.

### ***Commentary on the Template***

The template is provided as a tool for accountability agents. It is acceptable to depart from the template by reporting additional statistics. However, the core minimum statistics should be reported in each case since they will form a common and comparable minimum data set across all APEC Accountability Agent dispute resolution processes. In particular jurisdictions, governmental authorities may require the reporting of additional statistics.

### ***Complaint numbers***

The total number of complaints should be reported. Where no complaints are received, the complaint statistics template should be submitted indicating “none” to ensure it is clear that no complaints were received that year. A format for reporting will need to be adopted that makes clear the number of new complaints received as well as older complaints carried over from the previous reporting period.

To assist readers to understand the reported figures and to aid in comparability there should be a note as to how terms are being used. For instance, some matters may be on the borderline between an enquiry about a company’s information practice of concern and a complaint about that practice. Such matters may be quickly sorted out with an explanation to the enquirer or perhaps a telephone call to the company. Some programs may treat all matters as complaints while others may reserve that term for more formal dispute resolution or investigation and have another category for the matters treated less formally.

### ***Complaint outcomes***

This part of the template provides a picture of the processing of complaints.

### *Complaints type*

The template asks Accountability Agents to provide informative breakdowns of the complaints by type. This will provide a statistical picture of who is complaining and why.

Some complaints will raise several different issues. The report should explain the basis upon which the Accountability Agent is reporting. One approach is, for example, to identify the principal aspect of the complaint and treat it for statistical purposes as being only about that issue. An alternative is to count and classify all the allegations made in a complaint. If the latter approach is taken, the totals of complaint types will exceed the total number of complaints received and this will need to be explained or it may seem to be an anomaly.

### *Complaints process quality measures*

These statistics give a picture as to how well the complaints resolution system is working. At a minimum, some indication as to timeliness should be reported. At its simplest this might be to highlight the number of complaints that took longer than a target date to resolve (e.g. number of complaints on hand that are older than, say, three months) while some complaints systems may be able to produce a variety of more detailed statistics (e.g. the average time to resolve certain types of complaints). In a more sophisticated system other quality measures may be included and an Accountability Agent might, for example, report against internal targets or industry benchmarks if these are available.

### *General*

The Accountability Agent should comment on the various figures reported. To set the statistics in context, it is useful to include three or four years of figures where these are available.

## COMPLAINT STATISTICS TEMPLATE

### Complaint Numbers

Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number. A note should explain how the term ‘complaint’ is being used in the reported statistics.

### Complaint Processing and Outcomes

Complaints processed during the year broken down by the outcome.

Examples of typical outcomes include:

- complaints that could not be handled as they were outside the program’s jurisdiction (e.g. against a company that is not part of the CBPR program);
- complaints referred back to a business that are resolved at that point;
- complaints settled by the Accountability Agent;
- complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority;
- complaints for which the Accountability Agent has made a finding (such as complaint dismissed, complaint upheld in part, complaint upheld in full).

When the Accountability Agent has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action.

The Accountability Agent should include a comment on the significance of the complaints outcomes.

### Complaints Type

Further statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents. Useful

classifications will include:

- complaint subject matter broken down by APEC information privacy principle (notice, collection limitation, use, etc);
- basic information about complainants, where known, such as the economy from which complaints have been made;
- Information about the type of respondents to complaints – this will vary on the nature of a particular CBPR program but may include industry classification (e.g. financial service activities, insurance), the capacity in which the respondent falls (e.g. information processor, employer, service provider), or size of company (SME, large company etc).

The Accountability Agent should comment on the significance of the reported figures.

### **Complaints Process Quality Measures**

An indication should be given as to about any quality measures used in relation to the particular CBPR program. A typical measure may relate to timeliness. The Accountability Agent should offer a comment upon the figures reported.

## COMPLAINT STATISTICS FREQUENTLY ASKED QUESTIONS

Q. *Why does APEC require complaint statistics to be released?*

A. Complaints statistics are part of a transparent and accountable complaints handling system. The statistics will help paint a picture of how the CBPR program is operating. A number of stakeholders have an interest in seeing such a picture. For example, companies within a CBPR program, consumer advocates and regulators all have interest in knowing what happens in relation to the processing of complaints through an Accountability Agent. Transparency will promote understanding and confidence in the system.

Q. *Why do I need to release statistics on all the topics in the template?*

A. The template lists a minimum set of statistics that should be reported. To get a complete picture, all the categories of statistics are needed. Furthermore, since these are standard requirements across all APEC economies, the resultant statistics should be reasonably comparable. Over time, a picture should emerge as to how well CBPR programs are working and whether change is desirable.

Q. *How should these statistics be presented?*

A. The template provides the statistics that should be reported and requires that the Accountability Agent comment upon the significance of the figures. It is recommended that the statistics reported for a particular period should be published alongside the equivalent statistics for previous recent periods. Where available, three or four year's worth of figures should be reported. Accountability Agents are encouraged to put some effort into clearly displaying and explaining the statistics so that stakeholders can better appreciate their significance. For example, clear tables of figures with accompanying graphs are helpful.

Q. *Are there steps that can be taken to facilitate comparison across APEC jurisdictions?*

A. Accountability Agents are to include a classification in their reported statistics based on the APEC information privacy principles. This will aid comparison. In classifying respondents to complaints by industry type, it is recommended that the International Standard Industrial Classification of All Economic Activities (revised by the United Nations in 2008) be used or national or regional standards on industry classification that are aligned with that international standard. (See

<http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=27&Lg=1>



## **SIGNATURE AND CONTACT INFORMATION**

By signing this document, the signing party attests to the truth of the answers given.

---

**[Signature of person who has authority    [Date]**

**to commit party to the agreement]**

**[Typed name]**

**[Typed title]**

**[Typed name of organization]**

**[Address of organization]**

**[Email address]**

**[Telephone number]**

The first APEC recognition for an Accountability Agent is limited to one year from the date of recognition. Recognition for the same Accountability Agent will be for two years thereafter. One month prior to the end of the recognition period, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

**NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.**



## ACCOUNTABILITY AGENT APEC RECOGNITION APPLICATION FOR THE PRP SYSTEM

<i>Overview .....</i>	<i>2</i>
<i>Application Process .....</i>	<i>2</i>
<i>ANNEX A: Accountability Agent Recognition Criteria .....</i>	<i>3</i>
<i>ANNEX B: Accountability Agent Recognition Criteria Checklist .....</i>	<i>10</i>
<i>ANNEX C: APEC PRP Program Requirements Map .....</i>	<i>12</i>
<i>ANNEX D: Accountability Agent Complaint Statistics/Template/FAQs .....</i>	<i>22</i>
<i>ANNEX E: Signature and Contact Information .....</i>	<i>27</i>

## OVERVIEW

*The purpose of this document is to guide the application process for Accountability Agents seeking APEC recognition under the APEC Privacy Recognition for Processors (PRP) System. This document explains the necessary recognition criteria and provides the baseline program requirements of the PRP System. Only APEC-recognized Accountability Agents may participate in the PRP System. Once recognized, Accountability Agents may publicize this recognition and certify organizations as PRP-compliant.*

## APPLICATION PROCESS

In order to be considered eligible for recognition by APEC Economies, an Applicant Accountability Agent must:

- Explain how it is subject to the jurisdiction of the relevant enforcement authority in a PRP participating Economy<sup>1</sup>; *AND*
- Describe how each of the Accountability Agent Recognition Criteria (Annex A) have been met using the Accountability Agent Recognition Criteria Checklist (Annex B); *AND*
- Agree to make use of the template documentation developed and endorsed by APEC Economies (the PRP Intake Questionnaire, which includes questions to be answered by the applicant organization and baseline program requirements) against which the Accountability Agent would assess the applicant organization<sup>2</sup> when certifying organizations as PRP-compliant; *OR* demonstrate how their existing intake and review processes meet the baseline established using the PRP Program Requirements Map (Annex C); *AND*
- Complete the signature and contact information sheet (Annex F).

The completed signature and contact information sheet and all necessary supporting documentation should be submitted to the relevant government agencies or public authorities in any Economy in which the Applicant Accountability Agent intends to operate for an initial review to ensure the necessary documentation is included in the application, or other review as appropriate. The agency or authority may consult with other government agencies or authorities where necessary and will forward all information received to the Chair of the Electronic Commerce Steering Group, the Chair of the Data Privacy Subgroup and the Chair of the Joint Oversight Panel (JOP) where appropriate. The JOP will review the submitted information (and request any additional information that may be needed) when considering recommending the Applicant Accountability Agent for recognition by APEC Economies as an APEC PRP System Accountability Agent.

---

<sup>1</sup> An Economy is considered a participant in the Privacy Recognition for Processors System pursuant to the terms established in Paragraph 3.1 of the "Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel"

<sup>2</sup> Available at <https://cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf>

## ACCOUNTABILITY AGENT RECOGNITION CRITERIA

### CRITERIA

#### *Conflicts of Interest*

##### 1) General Requirements:

- a. An Accountability Agent must be free of actual or potential conflicts of interest in order to participate in the APEC Privacy Recognition for Processors (PRP) System. For the purposes of participation as an Accountability Agent in the PRP System, this means the ability of the Accountability Agent to perform all tasks related to an Applicant organization's certification and ongoing participation in the PRP System free from influences that would compromise the Accountability Agent's professional judgment, objectivity and integrity.
- b. An Accountability Agent must satisfy the APEC member economies with evidence that internal structural and procedural safeguards are in place to address potential and actual conflicts of interest. Such safeguards should include but not be limited to:
  - i. Written policies for disclosure of potential conflicts of interest and, where appropriate, withdrawal of the Accountability Agent from particular engagements. Such withdrawal will be required in cases where the Accountability Agent is related to the Applicant organization or Participant to the extent that it would give rise to a risk that the Accountability Agent's professional judgment, integrity, or objectivity could be influenced by the relationship.
  - ii. Written policies governing the separation of personnel handling privacy certification functions from personnel handling sales and consulting functions.
  - iii. Written policies for internal review of potential conflicts of interest with Applicant organizations and Participating organizations.
  - iv. Published certification standards for Applicant organizations and Participating organizations (see paragraph 4 'Program Requirements').
  - v. Mechanisms for regular reporting to the relevant government agency or public authority on certification of new Applicant organizations, audits of existing Participant organizations, and complaint processing.
  - vi. Mechanisms for mandatory publication of case reports in certain circumstances.

- 2) Requirements with respect to particular Applicant organizations and/or Participant organizations
- a. At no time may an Accountability Agent have a direct or indirect affiliation with any Applicant organization or Participant organization that would prejudice the ability of the Accountability agent to render a fair decision with respect to their certification and ongoing participation in the PRP System, including but not limited to during the application review and initial certification process; during ongoing monitoring and compliance review; during re-certification and annual attestation; and during complaint processing and enforcement of the Program Requirements against a Participant. Such affiliations, which include but are not limited to the Applicant organization or Participant organization and the Accountability Agent being under common control such that the Applicant organization or Participant organization can exert undue influence in the Accountability Agent, constitute relationships that require withdrawal under 1(b)(i).
  - b. For other types of affiliations that may be cured by the existence of structural safeguards or other procedures undertaken by the Accountability Agent, the existence of any such affiliations between the Accountability Agent and the Applicant organization or Participant organization must be disclosed promptly to the Joint Oversight Panel, together with an explanation of the safeguards in place to ensure that such affiliations do not compromise the Accountability Agent's ability to render a fair decision with respect to such an Applicant organization or Participant organization. Such affiliations include but are not limited to:
    - i. officers of the Applicant organization or Participant organization serving on the Accountability Agent's board of directors in a voting capacity, and vice versa;
    - ii. significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant organization or Participant organization, outside of the fee charged for certification and participation in the CBPR or PRP System; or
    - iii. all other affiliations which might allow the Applicant organization or Participant organization to exert undue influence on the Accountability Agent regarding the Applicant organization's certification and participation in the PRP System.
  - c. Outside of the functions described in paragraphs 5-14 of this document or those related to the CBPR certification of an Applicant or Participant, an Accountability Agent will refrain from performing for its Participants or Applicants services for a fee or any interest or benefit such as the following categories:
    - i. consulting or technical services related to the development or implementation of Participant organization's or Applicant organization's data privacy practices and procedures;

- ii. consulting or technical services related to the development of its privacy policy or statement; or
    - iii. consulting or technical services related to its security safeguards.
  - d. An Accountability Agent may be engaged to perform consulting or technical services for an Applicant organization or Participant organization other than services relating to their PRP and/or CBPR certification and on-going participation in the PRP and/or CBPR Systems. Where this occurs, the Accountability Agent will disclose to the Joint Oversight Panel:
    - i. the existence of the engagement; and
    - ii. an explanation of the safeguards in place to ensure that the Accountability Agent remains free of actual or potential conflicts of interest arising from the engagement [*such safeguards may include segregating the personnel providing the consulting or technical services from the personnel performing the functions described in paragraphs 5 -14 of this document and those related to the CBPR certification of an Applicant or Participant*].
  - e. Provision of services as required in Sections 3 through 6 shall not be considered performing consulting services which might trigger a prohibition contained in this document.
- 3) In addition to disclosing to the Joint Oversight Panel all withdrawals described above in Section 1(b)(i), an Accountability Agent also shall disclose to the Joint Oversight Panel those activities or business ventures identified in subsection 1(b) above that might on their face have been considered a conflict of interest but did not result in withdrawal. Such disclosures should include a description of the reasons for non- withdrawal and the measures the Accountability Agent took to avoid or cure any potential prejudicial results stemming from the actual or potential conflict of interest.

### ***Program Requirements***

- 4) An Accountability Agent evaluates Applicant organizations against a set of program requirements that encompass applicable principles of the APEC Privacy Framework with respect to processors and that meet the PRP System requirements developed and endorsed by APEC member economies (to be submitted along with this form, see Annex C). (*NOTE: an Accountability Agent may charge a fee to a Participant for provision of these services without triggering the prohibitions contained in paragraph 1 or 2.*)

### ***Certification Process***

- 5) An Accountability Agent has a comprehensive process to review an Applicant organization's policies and practices with respect to the Applicant organization's participation in the PRP System and to verify its compliance with the Accountability Agent's program requirements. The certification process includes:
  - a) An initial assessment of compliance, which will include verifying the contents of the self-assessment forms completed by the Applicant organization against the program requirements for Accountability Agents, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.
  - b) A comprehensive report to the Applicant organization outlining the Accountability Agent's findings regarding the Applicant organization's level of compliance with the program requirements. Where non-fulfillment of any of the program requirements is found, the report must include a list of changes the Applicant organization needs to complete for purposes of obtaining certification for participation in the PRP System.
  - c) Verification that any changes required under subsection (b) have been properly completed by the Applicant organization.
  - d) Certification that the Applicant organization is in compliance with the Accountability Agent's program requirements. An Applicant organization that has received such a certification will be referred to herein as a "Participant" in the PRP System.

### ***On-going Monitoring and Compliance Review Processes***

- 6) Accountability Agent has comprehensive written procedures designed to ensure the integrity of the Certification process and to monitor the Participant throughout the certification period to ensure compliance with the Accountability Agent's program.
- 7) In addition, where there are reasonable grounds for the Accountability Agent to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate review process will be triggered whereby verification of compliance will be carried out. Where non-compliance with any of the program requirements is found, the Accountability Agent will notify the Participant outlining the corrections the Participant needs to make and a reasonable timeframe within which the corrections must be completed. The Accountability Agent must verify that the required changes have been properly completed by the Participant within the stated timeframe.

### ***Re-Certification and Annual Attestation***

- 8) Accountability Agent will require Participants to attest on an annual basis to the continuing adherence to the PRP program requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-Certification. Where there has been a material change to the Participant's privacy policy (as reasonably determined by the Accountability Agent in good faith), an immediate review process will be carried out. This re-certification review process includes:
  - a) An assessment of compliance, which will include verification of the contents of the self-assessment forms updated by the Participant, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.
  - b) A report to the Participant outlining the Accountability Agent's findings regarding the Participant's level of compliance with the program requirements. The report must also list any corrections the Participant needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification.
  - c) Verification that required changes have been properly completed by Participant.
  - d) Notice to the Participant that the Participant is in compliance with the Accountability Agent's program requirements and has been re-certified.

### ***Complaint Processing Procedures***

9) An Accountability Agent must have a mechanism to receive and process complaints about Participants in relation to non-compliance with its program requirements, as well as a mechanism for cooperation on complaint processing with other Accountability Agents recognized by APEC economies when appropriate and where possible. An Accountability Agent may choose not to directly supply the complaint processing mechanism. The complaint processing mechanism may be contracted out by an Accountability Agent to a third party. Where the complaint processing mechanism is contracted out by an Accountability Agent the relationship must be in place at the time the Accountability Agent is recognized under the APEC PRP System.

10) Complaint processing, whether supplied directly or by a third party under contract, includes the following elements:

- a) A process for receiving complaints both from individuals and personal information controllers and determining whether a complaint concerns the Participant's obligations under the program and that the complaint falls within the scope of the program's requirements.
- b) A process for notifying the complainant of the determination made under subpart (a), above.



c) Where the complaint is from an individual and concerns the processing of his/her personal information and the Participant's obligations under the program:

i. A timely process for forwarding the complaint either (i) to the Participant and verifying that the Participant has forwarded it to the controller where the applicable controller can be identified or, where obligated by the controller, handled it directly; or (ii) to the applicable controller for handling.

ii. Written notice by the Accountability Agent or contracted third party supplier of the complaint processing service to the complainant and the Participant when the complaint has been forwarded.

iii. A process for obtaining an individual's consent before sharing that individual's personal information with the relevant enforcement authority in connection with a request for assistance.

d) A process for making publicly available statistics on the types of complaints received by the Accountability Agent or its third party contractor and how such complaints were processed, and for communicating that information to the relevant government agency and privacy enforcement authority (see Annex D).

### ***Mechanism for Enforcing Program Requirements***

11) Accountability Agent has the authority to enforce its program requirements against Participants, either through contract or by law.

12) Accountability Agent has a process in place for notifying Participant immediately of non-compliance with Accountability Agent's program requirements and for requiring Participant to remedy the non-compliance within a specified time period.

13) Accountability Agent has processes in place to impose the following penalties, which are proportional to the harm or potential harm resulting from the violation, in cases where a Participant has not complied with the program requirements and has failed to remedy the non-compliance within a specified time period. [NOTE: In addition to the penalties listed below, Accountability Agent may execute contracts related to legal rights and, where applicable, those related intellectual property rights enforceable in a court of law.]

a) Requiring Participant to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall remove the Participant from its program.

b) Temporarily suspending the Participant's right to display the Accountability Agent's seal.

c) Naming the Participant and publicizing the non-compliance.

d) Referring the violation to the relevant public authority or privacy enforcement authority. [NOTE: this should be reserved for circumstances

where a violation raises to the level of a violation of applicable law.]

- e) Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent.

14) Accountability Agent will refer a matter to the appropriate public authority or enforcement agency for review and possible law enforcement action, where applicable, where the Accountability Agent has a reasonable belief pursuant to its established review process that a Participant's failure to comply with the APEC PRP System requirements has not been remedied within a reasonable time under the procedures established by the Accountability Agent pursuant to paragraph 7 so long as such failure to comply can be reasonably believed to be a violation of applicable law.

15) Where possible, Accountability Agent will respond to requests from enforcement entities in APEC Economies that reasonably relate to that Economy and to the PPR-related activities of the Accountability Agent.

## **ACCOUNTABILITY AGENT RECOGNITION CRITERIA CHECKLIST**

### **Conflicts of Interest**

1. Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.
2. Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A.
3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

### **Program Requirements**

4. Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.

### **Certification Process**

5. Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d) of Annex A have been met.

### **On-going Monitoring and Compliance Review Processes**

6. Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d).
7. Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.

### **Re-Certification and Annual Attestation**

8. Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d) of Annex A.

### **Complaint Processing**

9. Applicant Accountability Agent should describe the mechanism to receive and process complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents that may be used when appropriate.
10. Applicant Accountability Agent should describe how the complaint processing meets the requirements identified in 10 (a) – (d) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third party

supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E.

### **Mechanism for Enforcing Program Requirements**

11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.
12. Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance.
13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.
14. Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].
15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

**APEC PRIVACY RECOGNITION FOR PROCESSORS SYSTEM  
PROGRAM REQUIREMENTS MAP**

SECURITY SAFEGUARDS .....	13
ACCOUNTABILITY MEASURES .....	17.

## SECURITY SAFEGUARDS

Question <i>(to be answered by the Applicant Organization)</i>	Assessment Criteria <i>(to be verified by the Accountability Agent)</i>	Relevant Program Requirement
1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify the existence of this written policy.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.</p>	
2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.	<p>Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include:</p> <ul style="list-style-type: none"> <li>• Authentication and access control (e.g. password protections)</li> <li>• Encryption</li> <li>• Boundary protection (e.g. firewalls, intrusion detection)</li> <li>• Audit logging</li> <li>• Monitoring (e.g. external and internal audits, vulnerability scans)</li> </ul>	

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
	<ul style="list-style-type: none"> <li>• Other (specify)</li> </ul> <p>The Applicant must periodically review and reassess these measures to evaluate their relevance and effectiveness.</p> <p>Where the Applicant indicates that it has <b>NO</b> physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.</p>	
<p>3. Describe how your organization makes employees aware of the importance of maintaining the security of personal information.</p>	<p>The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include:</p> <ul style="list-style-type: none"> <li>• Training program for employees</li> <li>• Regular staff meetings or other communications</li> <li>• Security policy signed by employees</li> <li>• Other (specify)</li> </ul>	

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
	Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	
4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that the existence of such measures is required for compliance with this principle.</p>	
5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	
6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's	The Accountability Agent must verify that the Applicant has in place appropriate processes to notify the controller of occurrences of a breach	



<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
personal information?	of the privacy or security of their organization's personal information.	
7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.</p>	
8. Does your organization use third-party certifications or other risk assessments? Please describe.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	

## ACCOUNTABILITY MEASURES

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
9. Does your organization limit its processing of personal information to the purposes specified by the controller?	The Accountability Agent must verify that the Applicant has policies in place to limit its processing to the purposes specified by the controller.	
10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?	The Accountability Agent must verify that the Applicant has measures in place to delete, update, and correct information upon request from the controller where necessary and appropriate.	
11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.	The Accountability Agent must verify that the Applicant indicates the measures it takes to ensure compliance with the controller's instructions.	
12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the PRP?	Where the Applicant answers <b>YES</b> , the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with the PRP.  Where the Applicant answers <b>NO</b> , the Accountability Agent must inform the Applicant that designation of such an	

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
	employee(s) is required for compliance with the PRP.	
13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant has procedures in place to handle, or forward to the controller as appropriate, privacy-related complaints or requests.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>	
14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information?	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant has procedures in place for notifying the controller, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject.</p> <p>Where the Applicant answers <b>NO</b>, the</p>	

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
	Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	
15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors?	The Accountability Agent must verify that the Applicant has in place a procedure to notify controllers that the Applicant is engaging subprocessors.	
16. Does your organization have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP? Please describe.	Where the Applicant answers <b>YES</b> , the Accountability Agent must verify the existence of each type of mechanism described.  Where the Applicant answers <b>NO</b> , the Accountability Agent must inform the Applicant that implementation of such mechanisms is required for compliance with this principle.	
17. Do the mechanisms referred to above generally require that subprocessors:	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
<p>a) Follow-instructions provided by your organization relating to the manner in which personal information must be handled?</p> <p>b) Impose restrictions on further subprocessing</p> <p>c) Have their PRP recognized by an APEC Accountability Agent in their jurisdiction?</p> <p>d) Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If <b>YES</b>, describe.</p> <p>e) Allow your organization to carry out regular spot checking or other monitoring activities? If <b>YES</b>, describe.</p> <p>f) Other (describe)</p>		

<b>Question (to be answered by the Applicant Organization)</b>	<b>Assessment Criteria (to be verified by the Accountability Agent)</b>	<b>Relevant Program Requirement</b>
18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.	<p>Where the Applicant answers <b>YES</b>, the Accountability Agent must verify that the Applicant has procedures in place for training employees relating to personal information management and the controller's instructions.</p> <p>Where the Applicant answers <b>NO</b>, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this requirement.</p>	

## **ACCOUNTABILITY AGENT COMPLAINT STATISTICS**

The Accountability Agent recognition criteria require applicant Accountability Agents to attest that as part of their complaint processing mechanism they have a process for releasing complaint statistics and for communicating that information to the relevant government agency and privacy enforcement authority.

The template, with associated guidance and FAQs will assist in meeting the requirement.

### ***Objectives of Reporting Complaint Statistics***

Complaints processing is an important element of the Privacy Recognition for Processors (PRP) program. The recognition criteria for Accountability Agents include an obligation to publish and report statistics on complaints received in order to:

- promote understanding about the operation of the PRP program;
- increase transparency across the PRP system;
- help governments, business and others to see how a complaints system is working and to help identify trends;
- enable comparisons of parts of the PRP program across the APEC region; and
- promote accountability of those involved in complaints processing and build stakeholder trust in Accountability Agents.

### ***Commentary on the Template***

The template is provided as a tool for Accountability Agents. It is acceptable to depart from the template by reporting additional statistics. However, the core minimum statistics should be reported in each case since they will form a common and comparable minimum data set across all APEC Accountability Agent complaint processing. In particular jurisdictions, governmental authorities may require the reporting of additional statistics.

#### ***Complaint numbers***

The total number of complaints should be reported. A format for reporting will need to be adopted that makes clear the number of new complaints received.

To assist readers to understand the reported figures and to aid in comparability there should be a note as to how terms are being used. For instance, some matters may be on the borderline between an enquiry about a company's information practice of concern and a complaint about that practice. Such matters may be quickly sorted out with an explanation to the enquirer or perhaps a telephone call to the company. Some programs may treat all matters as complaints while others may reserve that term for more formal complaints.

#### ***Complaint outcomes***

This part of the template provides a picture of the processing of complaints.

### *Complaints type*

The template asks Accountability Agents to provide informative breakdowns of the complaints by type. This will provide a statistical picture of who is complaining and why.

Some complaints will raise several different issues. The report should explain the basis upon which the Accountability Agent is reporting. One approach is, for example, to identify the principal aspect of the complaint and treat it for statistical purposes as being only about that issue. An alternative is to count and classify all the allegations made in a complaint. If the latter approach is taken, the totals of complaint types will exceed the total number of complaints received and this will need to be explained or it may seem to be an anomaly.

### *Complaints process quality measures*

These statistics give a picture as to how well the complaint processing system is working. At a minimum, some indication as to timeliness of complaint processing should be reported. At its simplest this might be to highlight the number of complaints that took longer than a target date to forward appropriately to the Participant or controller.

### *General*

The Accountability Agent should comment on the various figures reported. To set the statistics in context, it is useful to include three or four years of figures where these are available.



## COMPLAINT STATISTICS TEMPLATE

<b>Complaint Numbers</b>
<p>Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number. A note should explain how the term ‘complaint’ is being used in the reported statistics.</p>
<b>Complaint Processing and Outcomes</b>
<p>Complaints processed during the year broken down by the outcome.</p> <p>Examples of typical outcomes include:</p> <ul style="list-style-type: none"> <li>complaints that could not be handled as they were outside the program’s jurisdiction (e.g. against a company that is not part of the PRP program);</li> <li>complaints forwarded to the Participant;</li> <li>complaints forwarded to the applicable controller;</li> <li>complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority, where applicable;</li> </ul> <p>When the Accountability Agent has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action.</p> <p>The Accountability Agent should include a comment on the significance of the complaints outcomes.</p>
<b>Complaints Type</b>
<p>Further statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents.      Useful</p>

Classifications will include:

- complaint subject matter broken down by APEC information privacy principle (security safeguards and accountability);
- basic information about complainants, where known, such as the economy from which complaints have been made.
- Information about the type of respondents to complaints – this will vary on the nature of a particular PRP program but may include industry classification (e.g. financial service activities, insurance) or size of company (SME, large company etc).

The Accountability Agent should comment on the significance of the reported figures.

**Complaints Process Quality Measures**

An indication should be given about any quality measures used in relation to the particular PRP program. A typical measure may relate to timeliness. The Accountability Agent should offer a comment upon the figures reported.

## COMPLAINT STATISTICS FREQUENTLY ASKED QUESTIONS

- Q. *Why does APEC require complaint statistics to be released?*
- A. Complaints statistics are part of a transparent and accountable complaints processing system. The statistics will help paint a picture of how the PRP program is operating. A number of stakeholders have an interest in seeing such a picture. For example, companies within a PRP program, consumer advocates and regulators all have interest in knowing what happens in relation to the processing of complaints through an Accountability Agent. Transparency will promote understanding and confidence in the system.
- Q. *Why do I need to release statistics on all the topics in the template?*
- A. The template lists a minimum set of statistics that should be reported. To get a complete picture, all the categories of statistics are needed. Furthermore, since these are standard requirements across all APEC economies, the resultant statistics should be reasonably comparable. Over time, a picture should emerge as to how well PRP programs are working and whether change is desirable.
- Q. *How should these statistics be presented?*
- A. The template provides the statistics that should be reported and requires that the Accountability Agent comment upon the significance of the figures. It is recommended that the statistics reported for a particular period should be published alongside the equivalent statistics for previous recent periods. Where available, three or four years' worth of figures should be reported. Accountability Agents are encouraged to put some effort into clearly displaying and explaining the statistics so that stakeholders can better appreciate their significance. For example, clear tables of figures with accompanying graphs are helpful.
- Q. *Are there steps that can be taken to facilitate comparison across APEC jurisdictions?*
- A. Accountability Agents are to include a classification in their reported statistics based on the APEC information privacy principles. This will aid comparison. In classifying respondents to complaints by industry type, it is recommended that the International Standard Industrial Classification of All Economic Activities (revised by the United Nations in 2008) be used or national or regional standards on industry classification that are aligned with that international standard. (See <http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=27&Lg=1>)

## **SIGNATURE AND CONTACT INFORMATION**

By signing this document, the signing party attests to the truth of the answers given.

---

**[Signature of person who has authority    [Date]  
to commit party to the agreement]**

**[Typed name]**

**[Typed title]**

**[Typed name of organization]**

**[Address of organization]**

**[Email address]**

**[Telephone number]**

APEC recognition is limited to one year from the date of recognition. Each year one month prior to the anniversary of the date of recognition, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

**NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.**