



Making privacy core business

For OAIC:

Privacy Certification Research

Final

29 June 2020

Commercial-in-Confidence

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000, Australia



Table of Contents

- 1. Introduction 5
 - 1.1 Scope 5
 - 1.2 Caveats and limitations 5
- 2. Methodology 5
- 3. Privacy Certifications 6
 - 3.1 Singapore Data Protection Trust Mark 6
 - 3.1.1 Scope of certification and eligibility criteria 6
 - 3.1.2 Certification procedures and criteria 7
 - 3.1.3 Quality assurance 8
 - 3.1.4 Display and evidence of certification 9
 - 3.1.5 Role of accredited certification bodies 9
 - 3.1.6 Role of regulator 9
 - 3.1.7 Enforcement response 9
 - 3.1.8 Cost of certification 10
 - 3.2 New Zealand Privacy Trust Mark 10
 - 3.2.1 Scope of certification and eligibility criteria 11
 - 3.2.2 Certification procedures and criteria 11
 - 3.2.3 Quality assurance 11
 - 3.2.4 Display and evidence of certification 12
 - 3.2.5 Role of accredited certification bodies 12
 - 3.2.6 Role of regulator 13
 - 3.2.7 Enforcement response 13
 - 3.2.8 Cost of certification 13
 - 3.3 Japan PrivacyMark System 13
 - 3.3.1 Scope of certification and eligibility criteria 14



3.3.2	Certification procedures and criteria.....	14
3.3.3	Quality assurance.....	15
3.3.4	Display and evidence of certification	16
3.3.5	Role of accredited certification bodies.....	16
3.3.6	Role of regulator.....	18
3.3.7	Enforcement response	18
3.3.8	Cost of certification.....	19
3.4	APEC Cross Border Privacy Rules System.....	20
3.4.1	Scope of certification and eligibility criteria.....	20
3.4.2	Certification procedures and criteria.....	21
3.4.3	Quality assurance.....	21
3.4.4	Display and evidence of certification	23
3.4.5	Role of accredited certification bodies.....	23
3.4.6	Role of regulator.....	23
3.4.7	Enforcement response	24
3.4.8	Cost of certification.....	24
3.5	General Data Protection Regulation Certification Framework.....	25
3.5.1	Scope of certification and eligibility criteria.....	25
3.5.2	Certification procedures and criteria.....	26
3.5.3	Quality assurance.....	26
3.5.4	Display and evidence of certification	27
3.5.5	Role of accredited certification bodies.....	27
3.5.6	Role of regulator.....	27
3.5.7	Enforcement response	28
3.5.8	Cost of certification.....	29
4.	Interoperability	29

5. Appendix 1 – Key Documents Reviewed 30

 5.1.1 Singapore.....30

 5.1.2 New Zealand30

 5.1.3 Japan.....30

 5.1.4 APEC CBPR31

 5.1.5 GDPR.....32

6. Appendix 2 – Glossary of Key Terms 34

7. Appendix 3 – Table Summary of Certifications 35

1. Introduction

The Office of the Australian Information Commissioner (OAIC) has engaged Privcore to research five privacy certification frameworks and provide information relating to a number of identified areas of interest to the OAIC as outlined in this report. An additional Table Summary of Certifications with identified areas of interest (aside from quality assurance and certification procedures which is not conducive to summary tabular format) has also been included in Appendix 3.

1.1 Scope

The scope of this research covers the following five certification systems and frameworks:

- [Singapore Data Protection Trust Mark](#)
- [New Zealand Privacy Trust Mark](#)
- [Japan PrivacyMark System](#)
- [APEC Cross Border Privacy Rules System](#)
- [General Data Protection Regulation Certification Framework](#)

The OAIC has identified key issues to consider for each of the above systems and frameworks as addressed in this report. The OAIC may draw on this research to provide input to the review of the Privacy Act 1988 (Cth) taking place as a result of the ACCC's Digital Platform Inquiry's Final Report.

1.2 Caveats and limitations

Privcore has undertaken research to elucidate the main points to be addressed for each certification system and framework within scope. External consultation was not within scope; as such publicly available documents were relied upon in undertaking this research.

In relation to documents relating to the Japanese certification system, some documents were translated from Japanese to English using Google translate. As such, Privcore is not able to confirm the accuracy of any translations as it is out of scope (confidentiality-wise and price-wise) to send to Japanese privacy expert contacts for confirmation. Some documents were in English, but related only to high-level matters.

Privcore provides independent and objective privacy and risk management advice – It does not provide legal advice.

2. Methodology

The work was conducted between late May and June 2020. An initial document review was undertaken of a number of publicly available documents and materials about the certification frameworks and systems within scope. Relevant documents are outlined in Appendix 1. Subsequent to the initial document review, key points of interest to the OAIC were synthesised in this report. Prior to finalisation of this report, the OAIC was provided with a draft for comment.

3. Privacy Certifications

All certification frameworks within scope are voluntary and have been developed over timeframes ranging from 1998 to 2019. As such, they represent different levels of experience operating in their markets. The certifications at economy level have been presented in order of newest to oldest, commencing with Singapore, then New Zealand and Japan, prior to addressing APEC and EU-wide certification frameworks.

3.1 Singapore Data Protection Trust Mark

The Personal Data Protection Commission (PDPC) of Singapore developed the Data Protection Trust Mark (DPTM) and launched it in January 2019 after a trial period with eight organisations going through an assessment process in late 2018. The PDPC is part of the Infocomm Media Development Authority (IMDA) which administers the certification scheme. The CEO of IMDA is also the Personal Data Protection Commissioner: Mr Lew Chuen Hong. As at 10 June 2020, 30 organisations have been certified.

3.1.1 Scope of certification and eligibility criteria

The DPTM is an enterprise-wide certification covering the organisation’s standard of data protection policies, processes and practices. Singaporean private sector organisations, regardless of size and for-profit status that need to comply with the obligations of the Personal Data Protection Act 2012 (PDPA) can apply for a DPTM. Eligible organisations should be either:

1. formed or recognised under the laws of Singapore, or
2. resident, or having an office or a place of business, in Singapore, and in any case, not a public agency (as defined in the PDPA).

Source: [Terms and Conditions](#) between IMDA (Designated as the PDPC) and the eligible organization (the applicant) p.1.

[IMDA](#) suggests that organisations with ISO/IEC 27001 and 27701 may find it easier to attain DPTM certification as they have demonstrated good information security and privacy information management standards.

There are additional conditions for certain applicants in the following circumstances:

Circumstances	Conditions
(1) Previous application for the Certification was rejected	Application is made 3 months after IMDA’s notice of rejection of previous application
(2) DPTM Certification was previously revoked	Application is made 6 months after IMDA’s notice of revocation of previous certification
(3) Undergoing investigations by PDPC	Declaration of all investigations by PDPC within the 2 years prior to the date of application



(4) Previously found to have breached the PDPA	Declaration of all breaches under the PDPA within the 2 years prior to the date of application
--	--

Source: [Data Protection Trustmark Scheme Information Kit](#) p.6

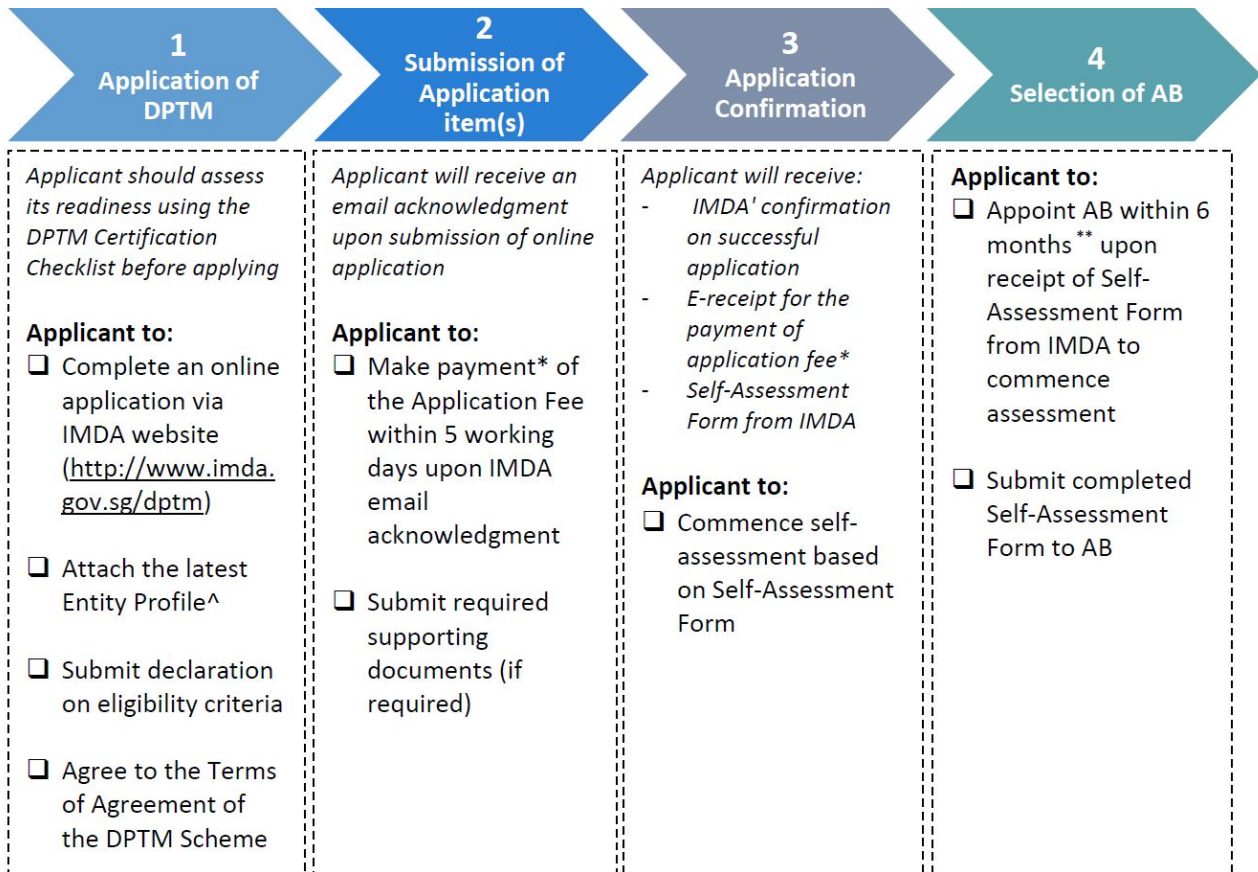
3.1.2 Certification procedures and criteria

The [certification criteria](#) have been developed based on a reflection of requirements in the PDPA, CBPR System and industry best practice. High level controls are based around four principles that need to be evidenced prior to award of certification:

1. Governance and Transparency
 - Appropriate policies and practices
 - Openness
 - Internal communication and training
2. Management of Personal Data
 - Appropriate purpose
 - Appropriate notification
 - Appropriate consent
 - Appropriate use and disclosure
 - Compliant overseas transfer
3. Care of Personal Data
 - Appropriate protection
 - Appropriate retention and disposal
 - Accurate and complete records
4. Individuals' Rights
 - Effect withdrawal of consent
 - Provide access and correction rights

A more detailed [certification checklist](#) accompanies the criteria which enables organisations to self-assess their readiness prior to applying for a certification. The checklist is comprised of 21 questions in total that relate to each of the above principles. The PDPC's guidance is referenced for each of those questions.

The application process for the certification occurs online. A high level overview of those procedures is in the following diagram which ends with the selection of the Assessment Body (AB in the diagram):



Source: [Data Protection Trustmark Scheme Information Kit](#) p.7

3.1.3 Quality assurance

The selection process to become an Approved Third-Party Assessment Body (Assessment Body) and retain that role is not publicly available, nor is it clear what liability attaches to those Assessment Bodies should a certified organisation later breach the PDPA, or otherwise compromise its certification. This is likely to depend on the contractual arrangements between the Assessment Body and the organisation seeking certification.

However, the certified organisation must notify IMDA of significant changes during the term of the certification. Such changes include change of ownership, changes to organisational structure and operations, products and services to which the certification applies. The full list is contained on p.21 of the [Data Protection Trustmark Scheme Information Kit](#). In addition, in accordance with clause 6 of the [Terms and Conditions](#) where the Certification Body (defined as IMDA (designated as the PDPC)), has reasonable grounds to suspect that a certified organisation has not complied with the terms and conditions or the PDPC has made a decision that the certified organisation has failed to comply with PDPA, the Assessment Body or other entity the Certification Body engages may need to conduct a review at the cost of the certified organisation. The Certification Body will determine whether the certification remains valid, is suspended, or terminated in the circumstances.

In accordance with clause 13 of the [Terms and Conditions](#), the Certification Body can suspend or terminate a certification held by an organisation. This would include circumstances that result in a breach of those Terms and Conditions, the provision of false or misleading information in



connection with the certification, or review necessitated by a significant change. Termination with immediate effect can occur in any of eleven scenarios as outlined in section 13.5. This importantly, includes where the Certification Body is of the view that the certified organisation: “does, or permits to be done, any act which might jeopardise or invalidate the registration of any Mark or does any act which might assist, or give rise to, an application to remove any Mark, or which might prejudice the legal right or title of the Certification Body to any Mark”. Additionally, in accordance with clause 10, the Certification Body can be indemnified for the breach and enforcement of those terms.

3.1.4 Display and evidence of certification

Certified organisations can display the DPTM’s image as shown in the summary table in Appendix 2. There is no unique certification number associated with the display logo for each certified organisation. IMDA maintains and publishes a full list of [certified organisations](#) and the validity period of their certification.

3.1.5 Role of accredited certification bodies

There are currently five accredited certification bodies, which are referred to as Approved Third-Party Assessment Bodies (Assessment Bodies), namely, [ISOCert](#), [Setsco Services](#), [TUV Sud](#), [BSI Group Singapore](#), [EPI Certification Pte Ltd](#). IMDA appointed ISOCert, Setsco Services and TUV Sud prior to launching the certification.

An assessment process takes between 2 and 4 months and involves the applicant submitting the IMDA’s self-assessment form to the selected Assessment Body, which then conducts an on-site verification. Where there are non-conformities, the applicant is given generally two months to rectify. The Assessment Body then completes its assessment report and evaluation and submits that to IMDA. IMDA reviews the assessment report and decides whether or not to issue the certification (including renewals when they fall due). There is no appeal process should a certification not be granted.

3.1.6 Role of regulator

The role of the regulator is central to the DPTM scheme, as it is the owner of the scheme and the organisation with which the certified organisation contracts, namely IMDA (designated as the PDPC). It is referred to as the Certification Body. An 18-page agreement outlines the [Terms and Conditions](#) for those participating in the scheme and holding a DPTM. Once an Assessment Body has assessed the organisation and IMDA has approved the certification, the Certification Body grants the organisation a license to use the DPTM as set out in those Terms and Conditions.

Once a certification is granted and there is a dispute relating to the certification or its use, the Certification Body will make a decision to address the dispute as outlined in section 25 of the [Terms and Conditions](#). The Certification Body’s decision regarding the dispute can be appealed to the Certification Appeal Committee, whose decision is final.

3.1.7 Enforcement response

There is no new or additional complaint handling mechanism for certified organisations. Nor is there any regulatory leniency provided to certified organisations. As such, the enforcement response is



the same for both certified and uncertified organisations. Certified organisations, though, are required to accept the [Terms and Conditions](#) of the DPTM scheme.

Importantly, the PDPC retains full regulatory power over the certified organisation, thus it cannot be used as a ticket to less regulatory oversight. This is spelled out clearly in clause 11 of the terms, as shown below:

The Applicant Organisation acknowledges and agrees that under no circumstances shall the Personal Data Protection Commission's powers under section 6 of the PDPA, including its powers to administer and enforce the PDPA, its subsidiary legislation, advisory guidelines and any other data protection-related rules and regulations, be hampered, limited or prejudiced in any way whatsoever.

For the avoidance of doubt, the Personal Data Protection Commission shall continue to have such powers under section 6 of the PDPA notwithstanding that the Applicant Organisation may (a) be assessed to fulfil the Certification Criteria, (b) be granted Certification, and/or (c) continue to comply with this Agreement and any other requirements of the Data Protection Trustmark Scheme.

Where the PDPC makes a determination or issues a decision that a certified organisation has failed to comply with the PDPA, the Certification Body may issue a notice under section 6 of the [Terms and Conditions](#). The Certification Body will obtain information as appropriate from the certified organisation, which must render full assistance to the Certification Body. The Assessment Body or other entity the Certification Body engages may be required to conduct a review at the cost of the certified organisation. The Certification Body will decide whether the certification shall remain valid, is suspended, or terminated.

3.1.8 Cost of certification

Currently there is a non-refundable \$S535 (inclusive of GST) application fee payable to IMDA. Until the end of 2020 the application fee is waived for small and medium enterprises and not-for-profits.

At 1 June 2020, the Assessment Body then charges fees between \$S1,400 and \$S10,000 plus GST depending on the size of the organisation seeking certification to conduct the assessment (regardless of whether the certification is granted). The Assessment Body determines the fees with any directions and guidelines as stipulated by the Certification Body as outlined in the Fees section of the [Terms and Conditions](#).

Eligible organisations can also apply to [Enterprise Singapore](#) or the [National Council of Social Services](#) to seek support for some of the costs for certification and optional consultancy services engaged to assist with readiness for certification.

The certification is for a three year term, with renewals required to be commenced at least six months before expiry. Renewal fees apply and assessment processes are required again for renewals. As outlined above, further assessments/audits may occur prior to certification expiry, should the Certification Body request this, for example, if a certified organisation is found in breach of the PDPA.

3.2 New Zealand Privacy Trust Mark

The Office of the Privacy Commissioner (OPC) in New Zealand developed the New Zealand Privacy Trust Mark (PTM) and launched it in May 2018. The PTM is awarded at the sole discretion of the



Privacy Commissioner, with no other assessment bodies involved. To date, five agencies have been awarded a PTM in relation to specific products and services. They are as follows:

- Air New Zealand – For its Privacy Centre which is a transparent, user-centric tool that gives customers control over their personal information in a proactive way
- Department of Internal Affairs – For RealMe which is a service that allows people to access multiple online services with one username and password, and securely prove who they are online
- Trade Me – For its Transparency Reporting which reports the requests it receives from government agencies, and its responses to those requests
- Trust, Integrity and Compliance Company’s (TICC) – For its anti-money laundering (AML) customer due diligence online forms and AML online portal
- Paperkite – For its contact tracing app called Rippl

The agencies and the product, service or process that has been awarded a PTM are listed on the OPC’s [website](#).

3.2.1 Scope of certification and eligibility criteria

The PTM is a certification for a product, service or process that warrants recognition for excellence in privacy. It is thus, not enterprise-wide, but can be given for multiple products and services within the one agency. Agencies are both private and public sector entities for the purposes of the New Zealand Privacy Act 1993.

3.2.2 Certification procedures and criteria

The [certification criteria](#) are based around seven key question areas that need to be evidenced prior to award of certification:

1. How is the product proactive about privacy?
2. Does the product/service demonstrate privacy by default?
3. Has privacy been embedded into its design?
4. Does it demonstrate end to end security?
5. Does it demonstrate the qualities of visibility and transparency?
6. Does it have respect for user privacy by putting the customer in control of their personal information?
7. Does it have user-centric features?

To apply, agencies must complete an application [form](#) detailing the privacy enhancing features of their product, service or process, as guided by the above seven questions. The application also requires a brief overview of the agency’s general privacy culture and practice, including its privacy policy, staff training, recent complaints and data breaches. Agencies need to address why they should be awarded a PTM.

3.2.3 Quality assurance

There are no assessment bodies, other than the Privacy Commissioner, appointed to issue the PTM. The PTM is awarded at the sole discretion of the Privacy Commissioner with no appeals



process. The [FAQs](#) clearly stipulate that the decision of the Privacy Commissioner on any application is final. If the Privacy Commissioner declines to award a PTM no further application can be made for that product, service or process for a period of at least six months. Some feedback may be provided (at the discretion of the Privacy Commissioner) when an application is not successful. Successful applications may have some information published, for example as outlined in the introduction in relation to Air New Zealand, Department of Internal Affairs, Trade Me, TICC and Paperkite.

During the two-year validity of the PTM if there are significant changes that could impact the PTM, such as the product, service or process ceasing to exist, changes in business operations which may affect the PTM, including website redesign, business rebranding or amendments to policies or material contracts, then notice of those changes must be made within 5 business days to the Privacy Commissioner in accordance with clause 3 of the [Terms and Conditions](#). The Privacy Commissioner will determine whether the certification remains valid in the circumstances.

In addition, in accordance with clause 4 of the [Terms and Conditions](#) certified agencies must promptly advise the Privacy Commissioner of:

- data breaches arising directly or indirectly from the certified product, service or process;
- warnings or public statements the agency issues in relation to the certified product, service or process and;
- any warnings, adverse findings, prosecution, litigation or other regulatory action adversely affecting the certified agency.

The Privacy Commissioner in accordance with clause 5 of the [Terms and Conditions](#) can suspend or terminate a certification held by an agency where the agency is in breach of the Terms and Conditions, a complaint is received, the agency brings the PTM into disrepute or the agency becomes insolvent. In accordance with clause 9, the Privacy Commissioner shall be indemnified for any loss, damage and expenses arising from the agency's use of the PTM.

3.2.4 Display and evidence of certification

Certified agencies can display the PTM's image as shown in the summary table in Appendix 3. The [Terms and Conditions](#) include brand guidelines and require that the PTM only be used in direct association with certified product, service or process. There is no unique certification number associated with the display logo for each certified agency. The OPC maintains and publishes a full list of [certified agencies](#) and the product, service or process that has been awarded the PTM, but not the validity period of their certification.

Agencies awarded a PTM must submit all marketing and promotional materials displaying the PTM to the Privacy Commissioner to approve as outlined in clause 8 of the [Terms and Conditions](#).

3.2.5 Role of accredited certification bodies

There are no accredited certification bodies. The Privacy Commissioner in their absolute discretion determines whether a PTM should be awarded.



3.2.6 Role of regulator

The Privacy Commissioner can award a PTM to a product, service or process identified as warranting recognition for excellence in privacy, thus an application is not always needed. Agencies can also apply to have a product, service, or process recognised with the PTM. Where a PTM is issued, the agency awarded a PTM (the Participant) must agree to [Terms and Conditions](#).

According to the [FAQs](#), the Privacy Commissioner will not audit agencies in relation to a PTM, though the Privacy Commissioner expects transparency in the assessment process, otherwise the application will be dismissed or the PTM revoked as the case may be.

3.2.7 Enforcement response

There is no new or additional complaint handling mechanism for certified agencies. Nor is there any regulatory leniency provided to certified agencies. As such, the enforcement response is the same for both certified and uncertified agencies. Certified agencies, though, are required to accept the [Terms and Conditions](#) of the PTM.

Importantly, the Privacy Commissioner retains full regulatory power over the certified agency, thus it cannot be used as a ticket to less regulatory oversight. This is spelled out clearly in clauses 2.4 and 10 of the terms, as shown below:

2.4 The Participant acknowledges that Accreditation does not mean that its obligations under the Privacy Act 1993, and other relevant legislation are met. The Participant is still responsible for ensuring that it meets its obligations under all relevant legislation.

10.2 The Programme and this agreement does not limit the exercise of the Privacy Commissioner's statutory functions in relation to any matter coming to his or her attention in connection with the Programme or this agreement.

10.3 The Privacy Commissioner may investigate complaints about the Participant under the Privacy Act 1993, including complaints about an accredited product, service or process, and may exercise his or her powers under the Privacy Act to obtain information from the Participant.

3.2.8 Cost of certification

The OPC does not impose an application or assessment fee for the PTM. The certification is for a two year term with renewals required to be commenced at least 60 days' before expiry.

3.3 Japan PrivacyMark System

The Japanese Institute for Promotion of Digital Economy and Community (JIPDEC) has been operating the PrivacyMark System (PrivacyMark) since 1998. JIPDEC is a [not-for-profit foundation](#) focused on the development of key IT technologies and policies. Since 2011 it has been a general incorporated foundation governed by the Act on Authorization of Public Interest Incorporated Associations and Public Interest Incorporated Foundations (Act No. 49 of 2006). The PrivacyMark was to some extent inspired by the introduction of the EU Data Protection Directive in 1995 and OECD Privacy Principles. The Ministry of Economy, Trade and Industry (METI) (formerly the Ministry of International Trade and Industry) had a 1997 'Guideline on the protection of personal



information processed by computer in the private sector' upon which the initial PrivacyMark was based. Subsequently when the standard, [JIS Q 15001 - Personal Information Protection Management System - Requirements](#) came out in 1999, it became the basis of the PrivacyMark certification.

As at 12 June 2020, [16,433 organisations](#) in Japan have current PrivacyMark certifications. One of the catalysts for the significant uptake of the PrivacyMark appears to have been the push by METI and government agencies to require organisations to obtain the certification before they can tender for, and be awarded, government contracts.

3.3.1 Scope of certification and eligibility criteria

Organisations eligible to apply for a PrivacyMark are generally private enterprises based in Japan. The certification is applied enterprise-wide and covers domestic operations only. It appears that more organisations than are regulated under the Japanese Act on the Protection of Personal Information (APPI) are able to apply for a PrivacyMark. APPI has a number of exclusions, such as broadcasting institutions, newspaper publishers, communications agencies, press organisations, writers, universities, political and religious bodies (in addition to government agencies that are not regulated under APPI as they are not business operators). See Articles 1, 2 and 76 of APPI.

Eligible organisations must have set up a Personal Information Protection Management System based on JIS Q 15001. There are also certain disqualification criteria, which would make an otherwise eligible entity, ineligible, including:

- Previous application or renewal has been rejected in the last three months
- Revocation or cancellation of PrivacyMark within a year of application
- Recent data breach or privacy incident
- Any executive of the applicant organisation has served a prison term or been suspended and less than two years has passed since end of sentence or suspension

Source: [Businesses that can apply for PrivacyMark qualification](#)

3.3.2 Certification procedures and criteria

JIPDEC has an extensive [PrivacyMark System Operating Procedure System](#) for all stakeholders involved in the System, including the examination bodies, the training requirements for examination bodies and their auditors.

Whilst the PrivacyMark is based on JIS Q 15001, it also [incorporates requirements](#) of APPI as amended and in force in 2017 including guidelines, local government ordinances relating to the handling of personal information and privacy requirements of industry groups. In some respects, JIS Q 15001 has broader coverage than APPI, for example, it also applies to personal information of deceased individuals.

The Privacy Mark questionnaire has over 100 questions and is a standard which is sold and subject to copyright and appears not to have a complete publicly available translation for purchase in English. At a high level the criteria follow a Plan, Do, Check, Act cycle and covers:



Plan

- Personal information protection policy
- Specification of personal information
- Laws, guidelines and other codes stipulated by the state
- Recognition, analysis and measures of risk
- Resources, roles, responsibility and authority
- Internal regulations
- Planning documents
- Preparation for state of emergency

Do

- Operation procedures
- Principles on acquisition, use and provision
- Appropriate control
- Rights of the person concerning personal information
- Education
- Personal information protection management system documents
- Response to complaints and consultations

Check

- Confirmation of operations
- Audits

Act

- Corrective actions and preventative actions
- Review by the representative of the business entity

Applicants should submit their application to the industry body to which they belong (the full list is under Role of Accredited Certification Bodies below). If the body is not available they can submit it to their specific regional body or JIPDEC. The application forms and instructions are available on JIPDEC's [website](#). The Certification Body then conducts an assessment of the documentation and conducts an on-site visit.

3.3.3 Quality assurance

There are a number of quality assurance measures built into the PrivacyMark System.

The PrivacyMark System Committee's main role is to establish and amend the standards and regulations to operate the PrivacyMark System, select and terminate Assessment Bodies and grant and revoke the use of the PrivacyMark. It is comprised of an external committee of nine members including individuals from academia, representatives of consumer and professional groups, privacy practitioners and lawyers.

There are also auditor quality standards and requirements for Assessment Bodies and training institutions set out in [extensive documentation](#).



Once a PrivacyMark is granted to an organisation there are obligations to advise the Assessment Body of changes to the organisation that may impact the PrivacyMark. For example, when an organisation merges or separates in accordance with Article 8 of the PrivacyMark [terms](#) or has a privacy incident in accordance with Article 11. In accordance with the [disqualification terms](#) privacy incidents include:

- Data leakage
- Data loss or damage
- Tampering
- Inaccuracy
- Unauthorised or inappropriate collection
- Unauthorised use or disclosure
- Refusal of requests for access
- Suspicion of any of the above

Such an event, however, is not expected to lead to automatic disqualification, though it is possible as outlined in Article 15 of the PrivacyMark [terms](#). Indeed, disqualification is extremely rare and requires the deliberation of the PrivacyMark System Committee. One instance where a PrivacyMark was [revoked](#) was in 2014 when [Benesse Holdings Inc](#), Japan's largest provider of distance education for children, suffered a privacy incident which compromised the personal information of millions of children.

Organisations in the process of obtaining a certification or those considering applying for a PrivacyMark also need to advise the Assessment Body of privacy incidents.

3.3.4 Display and evidence of certification

Certified organisations can display the PrivacyMark's image as shown in the summary table in Appendix 3. There is a unique certification number associated with the display logo for each certified organisation, which also incorporates a number reflecting the number of renewals. JIPDEC maintains and publishes a full list of [certified organisations](#), the validity period of their certification and their Assessment Body.

JIPDEC also publishes a list of [unauthorised organisations](#) using a PrivacyMark. JIPDEC may take legal measures where necessary if unauthorised organisations do not delete references to PrivacyMark certification.

3.3.5 Role of accredited certification bodies

There are a number of stakeholders that form part of the PrivacyMark System in addition to accredited certification bodies, known as Assessment Bodies. These additional stakeholders are as follows:

- PrivacyMark System Committee
 - (main role outlined in section 3.3.3 above)
- PrivacyMark Assessment Committee
 - (external committee that assesses reports from Assessment Bodies on PrivacyMark applicants and reports results to PrivacyMark System Committee)



- PrivacyMark Assessor Training Body
 - (external bodies that train assessors in Assessment Bodies)
- PrivacyMark Assessor Assessment Committee
 - (internal JIPDEC committee ensures assessors have the appropriate level of competence)
- PrivacyMark Assessor Registration Section
 - (within JIPDEC and operates registration of assessors)
- PrivacyMark Consumer Contact Committee
 - (within JIPDEC and each Assessment Body to handle inquiries and complaints about certified organisations)
- PrivacyMark Protest Assessment Committee
 - (ad hoc temporary committee within the PrivacyMark System Committee to handle complaints from certified organisations, applicants for the PrivacyMark, assessors in relation to their training or other complaints relating to the PrivacyMark System)

The Assessment Body granting use of the PrivacyMark is JIPDEC. It also conducts a significant portion of assessments. There are also 19 other entities which function as Assessment Bodies, including thirteen industry specific bodies and six regional bodies. JIPDEC selects the additional Assessment Bodies with approval of the PrivacyMark System Committee. They are limited to non-profit organisations and trade associations established by Japanese law in accordance with Article 7 of the [PrivacyMark System Basic Principles](#).

Industry specific bodies:

- Japan Information Service Industry Association [JISA]
- Japan Marketing Research Association [JMRA]
- Japan Association for the Study of Schools [JJA]
- Medical Information Systems Development Center [MEDIS-DC]
- All Japan Wedding and Mutual Funeral Association [All Mutual Cooperation]
- Japan Graphic Services Industry Association [JaGra]
- Japan Information Systems and Users Association [JUAS]
- Japan Data Communications Association [JADAC]
- Computer Software Association of Japan [CSAJ]
- Japan Printing Industry Federation [Nippon-Industry Federation]
- Broadcast Security Center [SARC]
- Mobile Content Forum [MCF]
- Japan LP Gas Equipment Inspection Association [LIA-AC]

Regional bodies:

- Kumamoto Industrial Support Foundation [KPJC]
- Chubu Sangyo Federation [Chusanren]
- Kansai Information Center [KIIS]
- Specified nonprofit corporation Michinoku Information Security Promotion Organization [TPJC]
- Hokkaido IT Promotion Association [DPJC]
- Chu-Shikoku Management System Promotion Organization [Chu-Shikoku MS Organization]



As at 31 March 2017, there were 1,246 individual assessors (including lead and provisional assessors). The individual assessors of the Assessment Bodies conduct the audits required to determine whether the PrivacyMark criteria are fulfilled by the applicant organisation.

In conducting their assessment, Assessment Bodies first conduct a document review comprised of verifying the content of the privacy policy, the Personal Information Management System (PMS) and procedure for its implementation. Second, an on-site visit is conducted to verify consistent implementation of the PMS, risk mitigation measures and whether the monitoring procedures have been set up. The Assessment Body's report is then drafted and provided to the PrivacyMark System Committee for review and approval.

JIPDEC and the Assessment Bodies through their Consumer Contact Committee also handle consumer inquiries and complaints regarding the certified organisations in relation to their handling of personal information. Where the certified organisation objects to the complaint, the PrivacyMark Protest Assessment Committee provides a report to JIPDEC which then decides the outcome and advises the certified organisation. The Protest Assessment Committee also deals with other complaints regarding assessors and training and outcomes of applications and renewals for a PrivacyMark. It is constituted as a temporary adhoc committee comprised of external experts.

3.3.6 Role of regulator

There is no formal role for the Personal Information Protection Commission (PPC) in Japan in relation to the PrivacyMark. Informally, [Dr Masao Horibe](#), former Chairperson of the PPC proposed and helped launch the PrivacyMark System. The PrivacyMark System was established before the APPI. Generally, the PrivacyMark has more requirements than the APPI.

PrivacyMark Assessment Bodies may be required to [report](#) privacy incidents to the [PPC](#). The procedures for reporting and where to submit reports are outlined extensively on JIPDEC's [website](#). Privacy incidents that are [reported](#) to the PPC generally relate to organisations that are **not** telecommunication carriers or broadcasters (those reports are sent to the Ministry of Internal Affairs and Communications) or where the PPC has delegated to a Ministry responsible for the field in which the organisation operates – then it is sent to the relevant government agency).

3.3.7 Enforcement response

Whilst there are extensive procedures and bodies and committees in place to administer the PrivacyMark System and certified organisations must agree to the PrivacyMark [terms](#), a PrivacyMark is rarely revoked. See p.16 of Moens and Crompton, Information Integrity Solutions "[Preliminary Assessment: Potential Benefits for APEC Economies and Businesses Joining the CBPR System](#)". This is despite hundreds of consumer complaints per year and reported privacy incidents.

When privacy incidents occur, the measures taken against the certified organisation range from no measures, to issuing advice, suspension and revocation of the PrivacyMark. The measure taken depends on the severity and cause of the privacy incident as outlined in the PrivacyMark System's [disqualification judgment criteria](#).



Each year JIPDEC publishes complaint statistics for the previous calendar year. The [latest version](#) published on 26 December 2019 relates to complaints received in 2018, of which there were 357 complaints. Since 2014, there have been no more than 422 complaints lodged in any one year. In 2018, 31.9% of complaints related to security of personal information and 12.9% related to disclosure of personal information. The provision of information and advice to respondents appears to be a common resolution to complaints.

Privacy incident and trend reports are also published annually. The latest [privacy incident and trend report](#) was published on 18 September 2019 in relation to 2018. There were 2,323 privacy incidents reported relating to 912 certified organisations in 2018. The most common privacy incidents were emails sent to unintended recipients (25.2%) and lost mail (20.6%) and wrong delivery address (14.9%). The intent of the reporting is to attempt to prevent and minimise future privacy incidents.

3.3.8 Cost of certification

A current price list is available on JIPDEC’s [website](#) and shown below. Costs are charged for the application, the assessment and the grant of the PrivacyMark to cover costs such as complaint management. Renewal applications are slightly discounted.

A PrivacyMark certification is valid for two years unless revoked prior due to, for example, a privacy incident. During the validity period should a privacy incident occur, an audit of the defect causing the privacy incident may occur in accordance with the PrivacyMark System’s [disqualification judgment criteria](#). Renewals may be applied for every two years thereafter. The renewal application must be made between four to eight months prior to the termination of the validity period in accordance with Article 9 of the PrivacyMark [terms](#).

Price list (Applied on October 1, 2019)

Unit: Yen (10% consumption tax included)

Type	When new			When updating		
	Business scale					
	Small scale	Medium scale	Large scale	Small scale	Medium scale	Large scale
Application fee	52,382	52,382	52,382	52,382	52,382	52,382
Examination fee	209,524	471,429	995,238	125,714	314,286	680,952
Granted registration fee	52,382	104,762	209,524	52,382	104,762	209,524
total	314,288	628,573	1,257,144	230,478	471,430	942,858

(100,000 yen = ~\$AU1,300)



Business scale is determined with reference to industry classification, revenue and number of employees. For not-profits, scale is only determined by the number of employees/contractors and is available on JIPDEC's [website](#).

3.4 APEC Cross Border Privacy Rules System

APEC Leaders endorsed the APEC Cross Border Privacy Rules System (CBPR System) in 2011. It was launched in July 2012 with the USA the first economy to sign up to the CBPR System. Additionally, in February 2015 APEC endorsed the Privacy Recognition for Processors (PRP), which is based on the CBPR System, but is designed for processors rather than controllers (in the GDPR context of those terms). References to the CBPR System below include references to the PRP. To date, 49 organisations have the CBPR System certification (including 14 as processors).

The CBPR System was built on the foundations of the [APEC Privacy Framework](#) and the [Cross Border Privacy Enforcement Arrangement](#) (CPEA). It is a voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies to facilitate trade. There are currently nine participating economies in the CBPR System, namely: USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei, and most recently the Philippines. The USA and Singapore are currently the only economies that have also [signed up](#) to the PRP.

The Asian Law Business Institute published at p.55 a [recent summary](#) of the status of the CBPR System in APEC economies including commentary on those economies with a possibility or interest in joining the CBPR System where they have not already joined.

3.4.1 Scope of certification and eligibility criteria

There are a number of conditions that must be satisfied as outlined in the [Charter](#) of the CBPR System and Joint Oversight Panel (JOP) prior to any certification processes. Namely, at least one privacy enforcement authority in the economy seeking to join is a participant in the CPEA; the economy intends to have at least one APEC recognised Accountability Agent; and the CBPR System can be enforced within the relevant economy. The JOP consists of representatives from three APEC economies for a two-year appointment. Its functions include making decisions on economies and Accountability Agents that meet the requirements to join the CBPR System.

One [further constraint](#) on eligibility is the scope of the privacy enforcement authorities remit. So, for example, in the USA, the Federal Trade Commission (FTC) is currently the only relevant privacy enforcement authority. It does not have jurisdiction over sectors including health, not-for-profit organisations and aspects of the financial services industry. Accordingly, organisations operating in these sectors cannot be part of the CBPR System as the Accountability Agent cannot operate in sectors outside the authority of the relevant privacy enforcement authority.

The scope of the certification is flexible and is determined by the organisation wishing to obtain a certification to participate in the CBPR System. It can be broad or narrow. The Intake questionnaire applicants submit includes provision for defining the scope, such as subsidiaries/ affiliates/ locations, data and processes within scope.

Examples of the scope selected by organisations certified to participate in the CBPR System include:



- narrow scopes, such as IBM, which has limited the certification to Customer/Applicant data only collected on www.ibm.com and that is further processed online or offline; and
- broad scopes, such as Rimini Street Inc, which includes Customer/Prospective Customer and Employee/Prospective Employee data collected online on all urls and offline for Rimini Street, Inc., Rimini Street Australia Pty Limited (Australia); Nihon Rimini Street KK (Japan), Nihon Rimini Street KK, Rimini Street de México, Rimini Street Singapore Pte. Ltd. Rimini Street Korea, Inc.

The CBPRs System's [website](#) lists the scope of each certification for each certified organisation. It can also be listed on the Accountability Agent's website. Commonly, certified organisation's seal or trustmarks as provided by the Accountability Agent will link back to the Accountability Agent's website, which also includes the scope of their client's certification, for example [TRUSTe](#).

3.4.2 Certification procedures and criteria

Organisations that are eligible to participate in the CBPR System need to submit to an audit by an APEC recognised Accountability Agent. The scope of the audit is defined by the organisation and provided in the [Intake questionnaire](#) they need to submit to the Accountability Agent. The Intake questionnaire has 50 questions plus sub-questions on how privacy is managed within the defined scope area. Questions cover notice, collection, use, choice, integrity, security, access and correction and accountability.

Subsequently, an [Intake questionnaire](#) was developed in 2015 designed for processors (in the European GDPR context of the term) limited to the security and accountability questions from the initial [Intake questionnaire](#). It consists of 18 questions plus sub-questions from the initial Intake questionnaire, again limited to the scope as the processor defines. Processor activities remain subject to enforcement through enforcement against the controllers as outlined in the [PRP purpose and background](#). This is because the CBPR System only applies to controllers. A controller and processor distinction is not an APEC Privacy Framework concept. Nevertheless, there was some demand for a processor-oriented certification.

Each Accountability Agent sets out on its own website its specific procedures and processes. Accountability Agents are required to use the CBPR System's Intake questionnaires and follow the [CBPR System's Program Requirements](#) or map their existing processes to the CBPR System [Program Requirements Map](#) when undertaking assessments. Accountability Agents that have published their procedures on their websites include:

- [JIPDEC](#) in Japan
- [IMDA](#) in Singapore
- [True Ultimate Standards Everywhere, Inc \(TRUSTe\)](#) in the USA
- [Schellman & Company, LLC \(Schellman\)](#) in the USA
- [NCC group](#) in the USA

3.4.3 Quality assurance

There are three main stakeholders involved in the management and governance arrangements of the CBPR System. The oversight body, the JOP, oversees the APEC recognised Accountability Agents and processes the applications of economies wishing to participate in the CBPR System.



APEC recognised Accountability Agents (which can be public or private sector entities) determine whether requirements for participating in the CBPR System have been met by organisations wishing to participate. They also handle consumer complaints about organisations they certify as being compliant with the CBPR System. Each economy participating in the CBPR System also has a privacy enforcement authority in the CPEA that can enforce the requirements of the CBPR System where the Accountability Agent fails to resolve issues.

The CBPR System has checks and balances in place for Accountability Agents when first joining the CBPR System, as well as annual reviews to ensure continued trust and effective operation as outlined in the [Accountability Agent application](#). Should an Accountability Agent only wish to certify processors, then it can use the Accountability Agent [processor application](#) which has similar quality assurance procedures.

When first joining the CBPR System, as outlined in the [Accountability Agent Application](#), the Accountability Agents need to:

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

The key selection criteria for Accountability Agents joining the CBPR System are summarised in the Accountability Agent Recognition Criteria Checklist found in Annex B of the [Accountability Agent Application](#). The selection criteria at a high-level are:

- Ensuring no conflicts of interest
- Identifying whether Accountability Agent intends to use APEC template documentation or adapt its existing processes to APEC program requirements
- Having appropriate certification process
- Ability to complete ongoing monitoring and compliance review processes
- Having a re-certification and review process
- Capability to handle complaints
- Ability to enforce APEC program requirements against certified organisations

Ongoing requirements for Accountability Agents to meet are outlined on the CBPR System's [website](#), and include obligations to ensure no conflicts of interest, ongoing monitoring of organisations it has certified, enforcing and reporting to privacy enforcement authorities on non-compliance by organisations where necessary and complaint statistic reporting requirements.

Additionally, anyone can report claims that an organisation is misrepresenting their participation in the CBPR System to cbprs@trade.gov as outlined on the CBPR System's [website](#).



3.4.4 Display and evidence of certification

Only organisations currently certified by an APEC recognised Accountability Agent may display a seal, trustmark, or otherwise claim to participate in the CBPR System. The Accountability Agent provides the relevant seals, as such they may differ between organisations depending on which Accountability Agent certified the organisation. Two examples of seals are provided in the table in Appendix 3, for the USA and Singapore.

The CBPR System's [website](#) lists the certified participating organisations in its compliance directory, split between controllers and processors. For each organisation, the following is displayed: the organisation name, scope of certification, their Accountability Agent, date of grant of certification and expiration/renewal date, economy and relevant privacy enforcement authority.

3.4.5 Role of accredited certification bodies

The accredited certification bodies in the CBPR System are known as Accountability Agents, which the JOP accredits. To date, there are six Accountability Agents, three of which have been actively certifying as listed under the first three bullet points below. The Accountability Agents are:

- TRUSTe in the USA (has certified 46 organisations to date)
- JIPDEC in Japan (has certified three organisations to date)
- IMDA in Singapore (has certified one organisation to date)
- Korea Internet and Security Agency in Korea
- Schellman in the USA
- NCC group in the USA

The Accountability Agents conduct audits and certify compliance with the CBPR System based on the relevant Intake questionnaire (for either controllers or processors) and their [obligations](#) as agreed to when they become APEC recognised Accountability Agents. They handle complaints from consumers in relation to organisations they have certified and have ongoing monitoring obligations to ensure compliance with the CBPR System. The complaint statistics are reported to the relevant government agency and privacy enforcement authority in line with Accountability Agent [obligations](#).

3.4.6 Role of regulator

The backbone of the CBPR System is the [CPEA](#), which enables privacy enforcement authorities to work together to resolve matters including where regional cooperation for enforcement may be required. Privacy enforcement authorities in the CPEA are also the backstop regulators for enforcing the CBPR System. This means that privacy enforcement authorities need to be able to enforce the requirements of the CBPR System. How this is done will vary in each economy. In Australia, it is likely that a [code would need to be developed](#) under the Privacy Act 1988 (Cth), as the CBPR System requirements in some places are more granular than the Australian Privacy Principles.

Generally, consumers lodge complaints first directly with the organisation certified, then the Accountability Agent and then the privacy enforcement authority, though there is no requirement to handle complaints in that order.



Whilst there are potential benefits to privacy enforcement authorities in having alternative dispute resolution pathways through Accountability Agents and further assurance processes in place, it is not clear whether a privacy enforcement authority would be more lenient towards an organisation participating in the CBPR System.

3.4.7 Enforcement response

The FTC which is the privacy enforcement authority in the USA, on occasion has taken action against organisations misrepresenting their participation in the CBPR System in the USA. Its [first action](#) was in 2016, and then subsequently against [three organisations](#) in 2017. Outcomes included settlements with consent arrangements prohibiting the misrepresentation.

Specific consumer complaints, however, do not appear to have reached the FTC, but have been handled by the key Accountability Agent, TRUSTe. The last published set of complaint statistics from TRUSTe show that there were [55 complaints](#) in the period 1 December 2015 to 28 February 2017. There is no requirement that Accountability Agents refer complaints to privacy enforcement authorities, as most of the time the Accountability Agent and certified organisation resolve the issue.

Japan and Singapore have more recently joined the CBPR System and it does not appear that complaints have reached their relevant privacy enforcement authorities.

Accountability Agents have a number of mechanisms available to rectify any non-compliance with the requirements of the certification as outlined in the [Accountability Agent Application](#). These include:

- Requiring the certified organisation to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall remove the certification.
- Temporarily suspending the certified organisation's right to display the Accountability Agent's seal.
- Naming the certified organisation and publicising their non-compliance.
- Referring the violation to the relevant public authority or privacy enforcement authority.
- Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent.

3.4.8 Cost of certification

The cost of certification to participate in the CBPR System varies between Accountability Agents and is dependent on the size of the organisation and the scope, as each organisation defines the scope of its certification which impacts pricing. The certification is valid for a one year period and renewable.

JIPDEC, the Accountability Agent in Japan is most transparent around [pricing](#). It has an examination fee for conducting the audit and reviewing the relevant Intake questionnaire – the average cost is around 666,657 yen (~\$AU8,700)(excluding consumption tax), but can vary



depending on the size of the organisation. It also has an annual certification management fee which is dependent on the certified organisation's previous year's revenue as follows:

- Revenue > 10 billion yen, fee is 1 million yen
- Revenue > 5 billion < 10 billion yen, fee is 500,000 yen
- Revenue > 1 billion < 5 billion yen, fee is 300,000 yen
- Revenue > 100 million < 1 billion yen, fee is 150,000 yen
- Revenue < 100 million yen, fee is 75,000 yen

The annual certification fee supports monitoring, ensuring ongoing compliance and complaint handling.

IMDA in Singapore encourages organisations to take up more than one certification (DPTM, CBPR, PRP) by enabling one application fee of \$535 (inclusive of GST) for multiple certifications in a single application process payable to IMDA. The [assessment fee](#) for the audit conducted by one of Singapore's approved Assessment Bodies, range between \$1,000 and \$8,000 (exclusive of GST) depending on the size of the organisation and scope of certification and is payable to the selected Assessment Body.

Eligible organisations can also apply to Enterprise Singapore to seek support for some of the costs for APEC CBPR certification and consultancy services.

3.5 General Data Protection Regulation Certification Framework

The General Data Protection Certification Framework is a nascent framework, with the backbone of its procedures, roles and obligations stipulated in the General Data Protection Regulation (GDPR). To date, certification criteria still need to be developed and certification bodies accredited. As such, there are currently no certifications operating under the GDPR. References to Articles in this section refer to Articles of the GDPR.

The key stakeholders involved in certification are accredited certification bodies and regulators, which include member state supervisory authorities and the European Data Protection Board (EDPB). Other stakeholders with fewer, but specifically, defined roles include; Member States, the EU Commission, and National Accreditation Bodies which are not within scope of this report.

3.5.1 Scope of certification and eligibility criteria

The certification scope can be broad or narrow and is dependent in part on certification criteria which are yet to be developed. It can be general or specific and apply, for example, to products, processes, services, systems, particular processes or the entire privacy program of a controller or processor. It can be offered in a particular Member State(s) or broadly across the European Union. The certification is intended for controllers and processors regulated by the GDPR.

According to the [Guidelines on Certification and Identifying Certification Criteria](#) in section 5.1, the main focus of certification is to help demonstrate compliance with the GDPR. The three core components that must be considered in the design of certification procedures and criteria are:

- personal data (material scope of the GDPR);



- technical systems - the infrastructure, such as hardware and software, used to process the personal data; and
- processes and procedures related to the processing operation(s).

Where a certification is designed to be EU-wide, known as a ‘European Data Protection Seal’, it still needs to be customisable for individual Member States to take into account Member State specific regulations where relevant, as expressed in section 4.2.2 of the above [Guidelines](#).

3.5.2 Certification procedures and criteria

There are currently no approved certification procedures and criteria or accredited certification bodies for issuing certificates under the GDPR. However, the [Guidelines on Certification and Identifying Certification Criteria](#) address at a high level what should be taken into account when drafting certification criteria where relevant, namely the:

- lawfulness of processing pursuant to Article 6,
- principles of data processing pursuant to Article 5,
- data subjects’ rights pursuant to Articles 12-23,
- obligation to notify data breaches pursuant to Article 33,
- obligation of data protection by design and by default, pursuant to Article 25,
- whether a data protection impact assessment, pursuant to Article 35(7)(d) has been conducted, if applicable; and
- technical and organisational measures put in place pursuant to Article 32.

Generally, in accordance with section 6 of the above [Guidelines](#) the following additional general considerations should be taken into account when defining certification criteria:

- be uniform and verifiable,
- auditable in order to facilitate the evaluation of processing operations under the GDPR, by specifying in particular, the objectives and the implementing guidance for achieving those objectives,
- be relevant with respect to the targeted audience (e.g. B2B and business to customer (B2C)),
- take into account and where appropriate be interoperable with other standards (such as ISO standards, national level standards); and
- be flexible and scalable for application to different types and sizes of organisations including micro, small and medium sized enterprises in accordance with Article 42(1) and the risk-based approach in accordance with Recital 77.

Additionally, the EDPB issued recent [Guidelines on the procedure for the approval of certification criteria which results in an EU-wide certification](#).

3.5.3 Quality assurance

Accredited certification bodies need to meet a number of criteria as outlined in Article 43(2). This includes demonstrating independence, expertise and no conflicts of interest, applying the relevant criteria in conducting assessments, have procedures to issue, review, withdraw certifications and handle complaints.



Additionally, section 6 of the [Guidelines on the accreditation of certification bodies](#) provide details of expectations of assessors (certification body personnel) qualifications.

Certification bodies will also need to consider changes that affect certifications, such as amendments to data protection legislation, relevant court decisions and decisions of the EDPB as outlined in section 7.10 of the above Guidelines.

3.5.4 Display and evidence of certification

In accordance with Articles 70(1)(o) and Article 42(8), the EDPB shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means. Additionally, it needs to maintain a public register of accredited bodies and certified controllers and processors established outside the EU. It does not address maintaining a register of certified controllers and processors within the EU. The EDPB has published a [register](#). However, there are no mechanisms, seals, marks, accredited bodies or certified controllers and processors established outside the EU listed in the register to date.

Under section 7.8 of the [Guidelines on the accreditation of certification bodies](#), the certification body will need to publish the following in relation to products/services it has certified:

- the scope of the certification and a meaningful description of the object of certification,
- the respective certification criteria (including version or functional status),
- the evaluation methods and tests conducted; and
- the result(s).

3.5.5 Role of accredited certification bodies

A certification pursuant to Article 42(5) shall be issued by the certification bodies referred to in Article 43, or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the EDPB pursuant to Article 63. Where the criteria are approved by the EDPB, this may result in a common certification, the European Data Protection Seal.

Under Article 42(7), certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not (or are no longer) met.

In accordance with Article 43(5) accredited certification bodies must provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

3.5.6 Role of regulator

Regulators include both supervisory authorities and the EDPB. When referring to regulators below, the author means supervisory authorities. However, it should be noted that the EDPB is able to undertake the same tasks as the supervisory authorities in the contexts below (though under different Articles), except for the issuing and withdrawing of certifications and publishing accreditation and certification criteria.

One of the tasks of the regulator under Article 57(1)(n) is to encourage the establishment of data protection certification mechanisms, data protection seals/marks and approve certification criteria. The regulator also has tasks to carry out periodic reviews of certifications under Article 57(1)(o), draft and publish the criteria for accreditation of a certification body and conduct the accrediting (Articles 57(1)(p) and (q)).

Regulators can also issue and withdraw certifications. Article 42(5) stipulates that “a certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the EDPB pursuant to Article 63. Where the criteria are approved by the EDPB, this may result in a common certification, the European Data Protection Seal.”

Further, Article 42(7) stipulates that “certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or no longer met.” The competent supervisory authority can also order the relevant accredited certification body to withdraw or not issue a certification to a particular applicant in accordance with Article 58(2)(h).

In accordance with Article 43(1)(a) Member States shall ensure that those certification bodies are accredited by the supervisory authority which is competent pursuant to Article 55 or 56. Certification bodies can also be accredited by the national accreditation body pursuant to Article 43(1)(b). This needs to be done in accordance with relevant regulations and standards and other requirements of the competent supervisory authority.

Under Article 43(4), accreditations are valid for a maximum of five years and may be renewed and revoked pursuant to Article 43(7) where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringes the GDPR.

The regulators’ powers to accredit certification bodies and issue certifications and approve certification criteria are also outlined under Article 58(3)(e) and (f).

3.5.7 Enforcement response

Whilst Article 42(4) provides that a certification does not reduce the responsibility of the controller or processor to comply with the GDPR and does not limit the tasks and powers of the relevant supervisory authorities, a certification can be used to demonstrate compliance in a number of areas of the GDPR.

For example, certifications can be used to demonstrate compliance with the:

- obligations of the controller under Article 24,
- requirements for privacy by design under Article 25,
- guarantees of the processor under Article 28,
- obligations to secure the processing of data under Article 32; and
- transfers of data to third countries with appropriate safeguards under Article 46

Further, adherence to certifications is a factor the relevant supervisory authorities can take into account when deciding to impose fines and the amount of those fines as per Article 83(2)(j).



Normally, one would expect a certification to be a mitigating factor, but as CIPL rightly points out in its paper on [‘Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms’](#) (p.10) it can be an aggravating factor 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.”

3.5.8 Cost of certification

Currently, there are no costs of certification published as no certifications have taken place under the GDPR certification framework. Under Article 42(7) certifications have a validity of maximum three years and may be renewed.

4. Interoperability

Considerations of interoperability have only recently begun, as many of the certification frameworks are relatively new.

The Singapore DPTM has been adapted from requirements under the Singapore PDPA, international benchmarks (including OECD and APEC) and best practices. It is [intended](#), therefore, to enable eligible organisations to more seamlessly obtain both the DPTM and the CBPR System certification. Indeed, this is facilitated through one application fee should an organisation wish to apply for more than one certification in a single application process. IMDA which administers the DPTM is also the Accountability Agent under the CBPR System, which is also helpful from an interoperability perspective.

There is no consideration of interoperability for the New Zealand PTM which is also relatively new. Japan, on the other hand has been operating a privacy certification framework, PrivacyMark, since 1998. JIPDEC issues the PrivacyMark certification and has also recently been appointed the Accountability Agent under the CBPR System. As such, there is potential scope for considerations of interoperability with other certification mechanisms.

Work commenced in 2013 to consider the interoperability between the CBPR System and Binding Corporate Rules (BCR) in the EU, the latter enables intra-company global data transfers. In contrast, the CBPR System enables data transfers between different organisations APEC-wide. A [common referential](#) was created to identify consistencies and gaps between the two frameworks. [Consideration](#) is also being given to opening up the CBPR System to non-APEC economies. ASEAN Members are also [considering interoperability](#) with the CBPR System as they develop an ASEAN cross-border data flow mechanism.

The GDPR certification framework is still in its infancy. There is nothing to preclude interoperability with other certification frameworks or standards. Certification criteria are yet to be developed so this is an area to watch.



5. Appendix 1 – Key Documents Reviewed

5.1.1 Singapore

IMDA and PDPC, [IMDA and PDPC launch pilot for Data Protection Trustmark certification scheme](#) undated

IMDA, [Agreement between the certification body and applicant organisation in relation to the data protection trustmark scheme](#), version at 22 August 2019

IMDA, [Data Protection Trustmark Certification](#) version at 18 June 2020

IMDA, [Data Protection Trustmark Scheme Information Kit](#), version at 7 April 2020

IMDA, [Overview of certification requirements](#), undated

IMDA, [DPTM certification checklist](#), version at December 2019

IMDA, [List of Data Protection Trustmark Certified Organisations](#), version at 10 June 2020

5.1.2 New Zealand

OPC, [Privacy Trust Mark Recipients](#) undated

OPC, [Criteria and Considerations](#) undated

OPC, [Privacy Trust Mark Application Form](#) undated

OPC, [Privacy Trust Mark FAQs](#) undated

OPC, [Privacy Commissioner's Privacy Trust Mark Accreditation Programme Terms and Conditions](#) undated

5.1.3 Japan

JIPDEC, [Search for businesses with privacy marks](#) as of 12 June 2020

JIPDEC, [Businesses that can apply for PrivacyMark qualification](#) 1 August 2018

JIPDEC, [PrivacyMark System Operating Procedure](#) 27 June 2019

JIPDEC, [What is the PrivacyMark System standard?](#) undated

JIPDEC, [New Application Method](#) undated

JIPDEC, [Operation point](#) 27 June 2019

JIPDEC, [PrivacyMark Terms](#) 1 July 2019

JIPDEC, [Disqualification matters and judgment criteria in the PrivacyMark System](#) 1 July 2019



- JIPDEC, [Unauthorised use of PrivacyMark \(logo\)](#) 10 April 2020
- JIPDEC, [PrivacyMark System Basic Principles](#) 1 July 2019
- JIPDEC, [Report of privacy incidents related to handling personal information](#) undated
- JIPDEC, [About reports such as privacy incidents](#) undated
- JIPDEC, [About privacy incidents regarding the handling of personal information](#) 22 April 2019
- JIPDEC, [Overview of 2018 consumer consultation service](#) 26 December 2019
- JIPDEC, [FY2018 Results of privacy incident report aggregation of handling personal information](#) 18 September 2019
- JIPDEC, [Cost](#) 1 October 2019
- JIPDEC, [Division of business size](#) undated
- Wikipedia, [JIS Q 15001](#) version at 2 July 2019
- Wikipedia, [Japan Institute for Promotion of Digital Economy and Community](#) version at 31 January 2020
- Nikkei Asian Review, [Customer data leak deals blow to Benesse](#) 10 July 2014
- Dr Masao Horibe, [Privacy Culture and Data Protection Laws in Japan](#) 2017 Data Protection and Privacy Commissioners' International Conference, Hong Kong
- Personal Information Protection Commission, [Correspondence such as leakage \(personal information\)](#) undated
- Moens and Crompton, Information Integrity Solutions, [Preliminary Assessment: Potential Benefits for APEC Economies and Businesses Joining the CBPR System](#) 2016
- #### 5.1.4 APEC CBPR
- APEC, [Privacy Framework](#) 2015
- APEC, [Cooperation Arrangement for Cross-border Privacy Enforcement](#) November 2019
- APEC, [Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel](#) November 2019
- APEC, [Cross-Border Privacy Rules System Intake Questionnaire](#) undated
- APEC, [Privacy Recognition for Processors Purpose and Background](#) undated
- APEC, [Accountability Agent APEC Recognition Application](#) November 2019
- APEC, [Accountability Agent APEC Recognition Application for the PRP System](#) undated



- APEC, [Cooperation Arrangements for Cross-Border Privacy Enforcement](#) August 2009
- Cross Border Privacy Rules System, [CBPR System Directory](#) at 8 June 2020
- Cross Border Privacy Rules System, [Ongoing APEC CBPR and PRP Systems Requirements for Accountability Agents](#) undated
- Cross Border Privacy Rules System, [Consumers](#) undated
- Cross Border Privacy Rules System, [CBPR Program Requirements](#) undated
- Cross Border Privacy Rules System, [CBPR Program Requirements Map](#) undated
- Federal Trade Commission, [Hand-held Vaporizer Company Settles FTC Charges It Deceived Consumers About Participation in International Privacy Program](#) 4 May 2016
- Federal Trade Commission, [Three Companies Settle FTC Charges that They Deceived Consumers About Participation in International Privacy Program](#) 22 February 2017
- JIPDEC, [CBPR Certification Examination Procedure](#) undated
- JIPDEC, [About the Cost](#) undated
- TRUSTe, [Rimini Street, Inc.](#) undated
- TRUSTe, [APEC CBPR and PRP Certifications](#) undated
- TRUSTe, [Complaint Statistics](#) undated
- IMDA, [APEC Cross Border Privacy Rules System](#) undated
- Schellman, [APEC Cross Border Privacy Rules Certification Process and Minimum Requirements](#) undated
- NCC Group, [APEC Privacy Certification](#) undated
- Asian Business Law Institute, [Transferring personal data in Asia: A path to legal certainty and regional convergence](#) May 2020
- Centre for Information Policy Leadership, [APEC CBPR & PRP Questions and Answers](#) March 2020
- Moens and Crompton, Information Integrity Solutions, [Preliminary Assessment: Potential Benefits for APEC Economies and Businesses Joining the CBPR System](#) 2016
- Moens and Crompton, Information Integrity Solutions, [Report for APEC: Australia – Phase 1 – CBPR – Impediment Analysis](#) 2014

5.1.5 GDPR

- European Data Protection Board, [Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation](#) 4 June 2019



European Data Protection Board, [Guidelines 4/2018 on the Accreditation of Certification Bodies under Article 43 of the General Data Protection Regulation](#) 4 June 2019

European Data Protection Board, [Procedure for the Approval of Certification Criteria by the EDPB Resulting in a Common Certification, the European Data Protection Seal](#) 28 January 2020

European Data Protection Board, [Register of Certification Mechanisms, Seals and Marks](#) undated

Centre for Information Policy Leadership, [Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms](#) 12 April 2017

6. Appendix 2 – Glossary of Key Terms

	Certification
CBPR System	APEC Cross Border Privacy Rules System
DPTM	Singapore Data Protection Trust Mark
PrivacyMark	Japan PrivacyMark System
PRP	APEC Privacy Recognition for Processors
PTM	New Zealand Privacy Trust Mark



	Accredited Certification Body
APEC (Asia-Pacific Economic Cooperation)	Accountability Agents 1) JIPDEC 2) IMDA 3) TRUSTe 4) Schellman 5) NCC Group 6) Korea Internet & Security Agency
Japan JIPDEC	Assessment Bodies Japanese Institute for Promotion of Digital Economy and Community 13 Industry specific bodies 6 regional bodies
Singapore	Approved Third Party Assessment Bodies 1) ISOCert 2) Setsco Services 3) TUV Sud 4) BSI Group Singapore 5) EPI Certification Pte Ltd


	Regulators, Government Authorities and Oversight Entities
EDPB	European Data Protection Board – Europe
FTC	Federal Trade Commission – USA
IMDA	Infocomm Media Development Authority – Singapore
JOP	Joint Oversight Panel – Three APEC economies (rotated)
METI	Ministry of Economy, Trade and Industry – Japan
OPC	Office of the Privacy Commissioner – New Zealand
PDPC	Personal Data Protection Commission – Singapore
PPC	Personal Information Protection Commission – Japan



	Legislation
APPI	Act on the Protection of Personal Information 2003 Japan (amended 2017)
GDPR	General Data Protection Regulation 2016/679 Europe
PDPA	Personal Data Protection Act 2012 Singapore



7. Appendix 3 – Table Summary of Certifications

Certification – seal as evidence of certification	Certification scope and eligibility criteria	Voluntary or Mandatory	Interoperability	Role of accredited certification body	Role of privacy regulator	Enforcement response	Cost of Certification
Singapore Data Protection Trustmark 	Enterprise-wide private sector organisations in Singapore	Voluntary	Alignment with APEC CBPR for controllers and processors. IMDA is Accountability Agent for APEC CBPR and certification approver for DPTM through PDPC.	IMDA (through PDPC) issues and renews certifications based on assessments undertaken by either: ISOCert, Setsco Services, TUV Sud, BSI Group Singapore or EPI Certification Pte Ltd.	IMDA (through PDPC) is the owner of the DPTM and provides licence to use mark when its terms and conditions are agreed to by organisation approved to have a certification.	No regulatory leniency provided to certified organisations. Where terms and conditions are breached, IMDA (through PDPC) can suspend or terminate certification.	3 year validity: Application fee: \$SG535 (inclusive of GST) Assessment Body fee: \$SG1,400 - \$10,000 plus GST
New Zealand Privacy Trust Mark 	Product, service or process of agency under the Privacy Act in New Zealand (both private and public sector entities)	Voluntary	Not interoperable	None	OPC assesses whether agency can be awarded certification and issues and renews certification. OPC provides licence to use mark when its terms and conditions are agreed to by agency approved to have a certification.	No regulatory leniency provided to certified agencies. Where terms and conditions are breached, OPC can suspend or terminate certification.	2 year validity: No fees

Certification – seal as evidence of certification	Certification scope and eligibility criteria	Voluntary or Mandatory	Interoperability	Role of accredited certification body	Role of privacy regulator	Enforcement response	Cost of Certification
<p>Japan PrivacyMark System</p>  <p>Unique Registration Number Underneath Seal</p>	<p>Enterprise-wide private sector organisations in Japan. Covers domestic operations only.</p>	<p>Voluntary</p>	<p>Not interoperable yet.</p> <p>JIPDEC is the Accountability Agent for APEC CBPR and certification approver for PrivacyMark.</p>	<p>JIPDEC issues and renews certifications based on assessments undertaken by either itself or one of 19 approved Assessment Bodies. JIPDEC has power to suspend or terminate certifications. JIPDEC is the owner of the PrivacyMark and provides licence to use mark when its terms of uses are agreed to by organisation approved to have a certification.</p>	<p>No formal role.</p> <p>Receives privacy incident reports from JIPDEC and other entities.</p>	<p>Complaint handling undertaken by JIPDEC and Assessment Bodies.</p> <p>Where terms of use are breached, JIPDEC can suspend or terminate certification. This is almost never done.</p>	<p>2 year validity:</p> <p>Below figures are yen and inclusive of consumption tax</p> <p>Initial Application: Application fee: 52,382 Assessment Body (examination) fee: 209,524 – 995,238 Granted certification fee: 52,382 – 209,524</p> <p>Renewal: Application fee: 52,382 Assessment Body (examination) fee: 125,714 – 680,952 Granted certification fee: 52,382 – 209,524</p>

Certification – seal as evidence of certification	Certification scope and eligibility criteria	Voluntary or Mandatory	Interoperability	Role of accredited certification body	Role of privacy regulator	Enforcement response	Cost of Certification
<p>APEC Cross Border Privacy Rules System Certification Framework</p>  	<p>Private sector organisations in APEC economies that participate in the CBPR System. Scope of certification determined by company seeking certification. Scope of certification published on cbprs.org website.</p>	<p>Voluntary</p>	<p>Work progressing on interoperability with the EU Binding Corporate Rules through a common referential. Consideration is also being given to opening up the CBPR System to non-APEC economies. ASEAN Members are also considering interoperability with the CBPR System as they develop an ASEAN cross-border data flow mechanism.</p>	<p>APEC recognised Accountability Agents issue and renew certifications based on Intake questionnaire and their auditing process. They monitor organisations' ongoing compliance with the CBPR System and handle complaints.</p>	<p>The privacy enforcement authorities are the backstop regulator to enforcing the CBPR System. They can also handle complaints from consumers regarding certified companies' potential non-compliance with the CBPR System.</p>	<p>No privacy enforcement authorities have handled complaints regarding the CBPR System, except the FTC in relation to entities misrepresenting they hold certification when they do not.</p>	<p>Varies depending primarily on Accountability Agent, scope of certification, and size of organisation.</p>
<p>General Data Protection Regulation Certification Framework</p>	<p>Controllers and processors regulated by the GDPR. Scope of certification determined by certification criteria to be drafted – can be narrow or broad and apply to specific products or processes or more broadly.</p>	<p>Voluntary</p>	<p>Criteria can be interoperable with existing standards and certifications – practical operation still to be determined.</p>	<p>Supervisory authorities and accredited certification bodies can issue, renew and withdraw certifications.</p>	<p>The supervisory authorities and the European Data Protection Board can encourage certifications, approve accreditation criteria for certification bodies and certification criteria. They can accredit certification bodies. Additionally, supervisory authorities can issue, renew and withdraw certifications when acting as a certification body.</p>	<p>Certification has no impact on obligations of controllers or processors or roles and powers of supervisory authorities. However, certifications can be used to help demonstrate compliance and may impact on the level of fines imposed in case of breach of the GDPR.</p>	<p>To be determined</p>

Commercial-in-Confidence

