TRPC Data Protection Index 2020

An assessment of 30 economies against the ASEAN Data Privacy Principles

TRPC

Table of Contents

Introduction

Data protection continues to be a growing concern for policymakers and consumers in the digital economy. As a result, many governments have put in place data protection frameworks and laws, such as data privacy laws, or personal data protection and privacy laws, in order to strengthen protection against the misuse and abuse of collected personal information. Some examples include the Australia Privacy Act 1988[1], the Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018[2], and the New Zealand Privacy Act 1993.[3]

In addition, a number of international and regional frameworks have developed to manage data protection,[4] such as the European Union's (EU) General Data Protection Regulation (GDPR) 2018, the Asia Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR) System 2011, and the Association of Southeast Asian Nations (ASEAN) Framework on Personal Data Protection 2016.

There have been some attempts to assess and measure how each jurisdiction has fared in strengthening their data protection regulations and laws. These include DLA Piper's database on the Data Protection Laws of the World,[5] Forrester's Global Heat Map of Privacy and Data Protection,[6] Commission Nationale de l'Informatique et des Libertés (CNIL) has published a heatmap on data protection around the world,[7] BestVPN's Privacy Index[8], and Comparitech's Surveillance States Index.[9]

The existing body of data protection assessments and indexes make assumptions on what a strong data protection regime comprises.[10] For example, Forrester's Global Heat Map on Privacy and Data Protection tracks "government surveillance" as it deems that this may impact privacy. Comparitech assesses "visual surveillance", as well as "democratic safeguards" such as freedom of speech in the country, and journalist protections. BestVPN grades countries against the EIU's Democracy Index. CNIL's heatmap on data protection around the world assesses countries according to adequacy with the EU GDPR.

These factors – evidence of free speech and democracy, or adequacy with the EU GDPR – may not be universally accepted by countries as evidence for or against a strong data protection regime.

The inaugural TRPC Data Protection Index 2020 (DPI 2020) is the first index to establish an objective, data protection assessment mechanism. Based on the seven Principles of Personal Data Protection in the ASEAN Framework on Personal Data Protection 2016, it poses 12 questions to assess an economy's data protection laws and regulatory environment. Economies are then scored against these questions, to derive an overall score that demonstrates if it has a strong data protection regulatory environment.

In this first iteration of the DPI, 30 economies have been scored. To enable policymakers to conduct comparisons on a national and international level, these countries include all economies represented in ASEAN (10 member states),[11] APEC (21 member economies),[12] and the G20 (20 member economies).[13]

[1] https://www.oaic.gov.au/privacy/the-privacy-act/
[2] https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf
[3] http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html
[4] See Appendix C for more detail.
[5] https://www.dlapiperdataprotection.com/
[6] https://heatmap.forrestertools.com/
[7] https://www.cnil.fr/en/data-protection-around-the-world
[8] https://bestvpn.org/privacy-index/
[9] https://www.comparitech.com/blog/vpn-privacy/surveillance-states/
[10] See Appendix B for more detail.
[11] https://asean.org/asean/asean-member-states/
[12] https://www.apec.org/About-Us/About-APEC/Member-Economies
[13] https://g20.org/en/about/Pages/Participants.aspx

TRPC Data Protection Index 2020 (DPI 2020)

The DPI 2020 seven Principles of Personal Data Protection in the ASEAN Framework on Data Protection 2016[14] to assess the level of data protection across various economies. This is the first index to use the ASEAN Framework on Data Protection as a best practice guideline, where the assessment of a positive data protection policy posture by a country would be one which promotes the free flow of data across borders.

ASEAN Framework on Personal Data Protection 2016: Principles of Personal Data Protection

The Association of Southeast Asian Nations (ASEAN) developed the Framework on Personal Data Protection, released in 25 Nov 2016.[15] The framework comprises seven Principles of Personal Data Protection:

1. **Consent, Notification and Purpose** – (a) an organisation should not collect, use or disclose personal data about an individual unless: (i) the individual has been notified of and given consent to the purpose(s) of the collection, use or disclosure of his/her personal data; or (ii) the collection, use or disclosure without notification or consent is authorised or required under domestic laws and regulations, and (b) an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.

2. **Accuracy of Personal Data** - the personal data should be accurate and complete to the extent necessary for the purpose(s) for which the personal data is to be used or disclosed.

3. **Security Safeguards** - the personal data should be appropriately protected against loss and unauthorised access, collection, use, disclosure, copying, modification, destruction or similar risks.

4. **Access and Correction** - upon request by an individual, an organisation should: (i) provide the individual access to his/her personal data which is in the possession or under the control of the organisation within a reasonable period of time; and (ii) correct an error or omission in his personal data, unless domestic laws and regulations require or authorise the organisation not to provide access or correct the personal data in the particular circumstances.

5. **Transfers to Another Country or Territory** - before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles.

6. **Retention** - an organisation should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes.

7. **Accountability** – (a) an organisation should be accountable for complying with measures which give effect to the Principles, and (b) an organisation should, on request, provide clear and easily accessible information about its data protection policies and practices with respect to personal data in its possession or under its control. An organisation should also make available information on how to contact the organisation about its data protection policies and practices.

[14] https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf
[15] https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf

Methodology and Assessment Questions

The DPI 2020 assessment comprises 12 questions.[16] It starts by establishing the existence of a data protection law and a privacy enforcement authority (PEA), and follows with questions that operationalise the seven ASEAN Principles of Data Protection into 12 questions and scored according from 6 (strong data protection) to 0 (no data protection).

The scoring also allows for some nuances; for instance where there are draft laws which have yet to be passed, or where there is evidence that the data protection principle is protected in another legislation or regulation which may not be in the data protection law. The assessment concludes with two final questions on whether the economy's is a participant in the EU GDPR, APEC CBPR, or similar regional data protection framework.

The DPI 2020 questions are as follows:

1. Does the economy have a personal data protection law?

2. Does the economy have a privacy enforcement authority (PEA)?

3. ***[ASEAN Principle 1. Consent, Notification and Purpose]*** Does the personal data protection law require that organisations obtain consent from individuals, and notify them of the purposes of collection, use, and disclosure of their personal information by the organization?

4. ***[ASEAN Principle 1. Consent, Notification and Purpose]*** Does the personal data protection law have clear instructions on exemption circumstances by which consent from individuals for the collection, use, and disclosure of their personal information, is NOT required? E.g. where collection of personal information is authorised or required under domestic laws and regulations?

5. ***[ASEAN Principle 2. Accuracy of Personal Data]*** Does the personal data protection law require organisations to ensure that personal data be accurate and complete for the extent necessary for the purpose(s) for which the personal data is to be used or disclosed?

6. ***[ASEAN Principle 3. Security Safeguards]*** Does the personal data protection law require that personal data be appropriately protected against loss and unauthorised access, collection, use, disclosure, copying, modification, destruction or similar risks?

7. ***[ASEAN Principle 4. Access and Correction]*** Does the personal data protection law require organisations to, upon request from individuals, provide the individual access to his/her personal data which is in the possession or under the control of the organisation within a reasonable period of time, and correct an error or omission in his personal data, unless domestic laws and regulations require or authorise the organisation not to provide access or correct the personal data in the particular circumstances?

8. ***[ASEAN Principle 5. Transfers to Another Country or Territory]*** Does the law require that, before transferring personal data to another country or territory, the organisation should obtain the consent of the individual for the overseas transfer?

9. ***[ASEAN Principle 6. Retention]*** Does the personal data protection law require that an organisation cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes, or after a certain period of time (e.g. 5 yrs)?

10. ***[ASEAN Principle 7. Accountability]*** Does the personal data protection law require an organisation to, on request, provide clear and easily accessible information, such as how to contact the organisation, about its data protection policies and practices with respect to personal data in its possession or under its control?

11. Is the economy a participant of the EU's GDPR regime, or meets GDPR adequacy requirements?

12. Is the economy a participant of the APEC CBPR or similar regional system (promoting an accountability rather than an adequacy system)?

[16] See Appendix A for full questionnaire and scoring mechanism.

Results

The table below shows the ranks and scores across 30 economies.[17]

MARKET	Q1 Data protection (DP) law?	Q2 Privacy enforcement authority (PEA)?	Q3 Consent required for collection, use, discloser of personal info?	Q4 Does DP law allow for exemptions?	Q5 Does PD law require data to be accurate and complete for its purpose of collection?	Q6 Does PD law require appropriate security safeguards?	Q7 Does PD law allow the individual to access and correct his data?	Q8 Does the PD law require consent for overseas transfer of data?	Q9 Does the PD law provide legal limits to retaining data (right to be forgotten)?	Q10 Does the PD law require the collecting organisation to provide clear data collection policies, and a contact point for queries?	Q11 EU GDPR participant/adequate?	Q12 APEC CBPR participant/similar accountability mechanism?	Total Score	Normalized	Rank
Japan	6	6	6	6	6	6	6	6	6	6	6	6	**72**	**10.0**	**1**
South Korea	6	6	6	6	6	6	6	6	6	6	2	6	**68**	**9.4**	**2**
United States*	5	2	6	6	6	6	6	6	6	6	6	6	**67**	**9.3**	**3**
Australia	6	6	6	6	6	6	6	6	6	6	0	6	**66**	**9.2**	**=4**
Estonia	6	6	6	6	6	6	6	6	6	6	6	0	**66**	**9.2**	
Germany	6	6	6	6	6	6	6	6	6	6	6	0	**66**	**9.2**	
Mexico	6	6	6	6	6	6	6	6	6	6	0	6	**66**	**9.2**	
Singapore	6	6	6	6	6	6	6	6	6	6	0	6	**66**	**9.2**	
United Kingdom	6	6	6	6	6	6	6	6	6	6	6	0	**66**	**9.2**	
Brazil	6	6	6	6	6	6	6	6	6	6	0	0	**60**	**8.3**	**=10**
Canada	6	6	6	6	6	6	6	0	6	6	6	0	**60**	**8.3**	
Hong Kong	6	6	6	6	6	6	6	6	6	6	0	0	**60**	**8.3**	
Malaysia	6	6	6	6	6	6	6	6	6	6	0	0	**60**	**8.3**	
New Zealand	6	6	6	6	6	6	6	0	6	6	6	0	**60**	**8.3**	
Peru	6	6	6	6	6	6	6	6	6	6	0	0	**60**	**8.3**	
Russia	6	6	6	6	6	6	6	6	6	6	0	0	**60**	**8.3**	
South Africa	6	6	6	6	6	6	6	6	6	6	0	0	**60**	**8.3**	
Taiwan	6	6	6	6	6	6	6	0	6	6	0	6	**60**	**8.3**	
Thailand	6	6	6	6	6	6	6	6	6	6	0	0	**60**	**8.3**	
UAE*	6	6	6	6	6	6	6	6	6	6	0	0	**60**	**8.3**	
Brunei	2	6	6	6	6	6	6	6	6	6	0	0	**56**	**7.8**	**=21**
Philippines	6	6	6	6	6	6	6	0	6	6	0	2	**56**	**7.8**	
India*	4	0	6	6	6	6	6	6	6	6	0	0	**52**	**7.2**	**23**
Indonesia*	4	0	6	0	6	6	6	6	6	6	0	0	**46**	**6.4**	**24**
Chile	6	0	6	6	6	6	6	0	6	0	0	0	**42**	**5.8**	**25**
Vietnam	2	0	2	2	2	2	2	0	2	2	0	0	**16**	**2.2**	**26**
China	2	0	2	2	0	2	2	0	2	2	0	0	**14**	**1.9**	**27**
Laos*	2	0	2	0	0	2	0	0	0	0	0	0	**6**	**0.8**	**28**
Cambodia	2	0	0	0	0	2	0	0	0	0	0	0	**4**	**0.6**	**29**
Myanmar	2	0	0	0	0	0	0	0	0	0	0	0	**2**	**0.3**	**30**

Average score = 8.3
Median = 6

[17] * The scores for India and Indonesia are based draft laws which have not been officially passed yet. For the United States, the EU-US Privacy Shield Framework has been used for the purpose of assessing data privacy. For the UAE, the Dubai Data Protection Law (DIFC Law No. 1 of 2007) was used. For Laos, no English translation was available for the Laos Electronic Data Protection Law (EDPL) which was only available officially as a scanned non-machine-readable copy, and therefore scores are based on data from Data Guidance: https://free.dataguidance.com/laws/laos-electronic-data-protection-law

Observations

Top scorers have established and/or explicit data protection policies

The scores show that there is a general band of markets who have good to excellent data protection scores, where they scored 6 or above (the median score). These countries tend to be countries who have established data protection laws or policies.

The existence of a law or policy which can demonstrably prove that the principles of data protection are protected in an economy is therefore of paramount importance. All economies which scored 6 and have an existing data protection law or policy in place.

The exceptions are USA - which has the EU-US Privacy Shield Framework in place, Brunei, which has a data protection policy, and India and Indonesia, which have draft data protection policies in place.

Top scorers have strong local data protection laws, and good international participation

The scores reveal that top scoring economies tended to have strong data protection policies in place locally, while also participating in international data protection regimes and mechanisms.

For example, Japan (#1) and South Korea (#2) both have established data protection laws and enforcement agencies, and are both participating in the APEC CBPR system, as well as applied to be recognized under the EU's GDPR adequacy requirements. Japan pips South Korea in this respect, as it received the first adequacy decision by the EU GDPR in Jan 2019, while South Korea's application has yet to be approved.

Scoring tends to "band"

Most economies studied tended to band around two scores - 9.2/equal 4th rank (6 markets), or 8.3/equal 10th rank (11 markets). This observation shows that data protection laws have developed some standard principles which are well-protected amongst most economies.

For example, Australia, Estonia, Germany, Mexico, Singapore, and the United Kingdom all score equal 4th, and the only differences in their scorings relate to whether or not they are participating in the EU GDPR or the CBPR mechanisms.

ASEAN economies could use the ASEAN Privacy Principles to establish a baseline data protection policy or law

Half of ASEAN member states fall in the lower ranks of the DPI 2020, which suggests that there is still work that needs to be done to improve data protection within the region. There is a great opportunity for the ASEAN region to work together to improve their policies together.

This report thus offers an approach unique to ASEAN. Through the DPI 2020, it offers an approach towards designing a data protection law which is built on the seven principles of the ASEAN Principles of Data Protection, which may be followed by ASEAN member states when drafting their data protection laws.

Market Briefs

Australia [9.2/=4th]
Australia has been one of the leaders in Asia Pacific data protection laws and continues to improve consumer data protection and privacy through organisations such as the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC).

Brazil [8.3/=10th]
A data protection market leader in South America which is leading the way for its neighbours.

Brunei [7.8/=21st]
Brunei is notable as it has an established Data Protection Policy established in 2014 and enforced by the E-Government National Centre, under the Prime Minister's Office. However, it remains as a policy, and not a law, which may be the market's next step in strengthening its data protection regulations.

Cambodia [0.6/29th]
While citizens' right to privacy are granted under the Cambodian constitution, the state has yet to develop a data protection law.

Canada [8.3/=10th]
A global leader in privacy laws, Canada has strived to develop a strong business environment that allows companies to trade internationally.

Chile [5.8/25th]
Chile is unusual in that it has an established data protection law, but no central regulator for it. Instead, its laws are enforced by the courts.

China [1.9/27th]
No data protection law exists, although some provisions for its aspects may be found in its cybersecurity law.

Estonia [9.2/=4th]
A member of the EU, Estonia's data protection laws aligns with the EU GDPR.

Germany [9.2/=4th]
A member of the EU, Germany's data protection laws aligns with the EU GDPR. However, Germany is unusual in that the enforcement of data protection takes place on a state level, where all 16 of its states work to enforce data protection.

Hong Kong [8.3/=10th]
One of the leading Asian states with a strong data protection law, and an established data protection agency.

India [7.2/23rd]
India's data protection is expected to improve once its draft Personal Data Protection Bill 2018 is passed in Parliament (expected in 2020.)

Indonesia [6.4/24th]
Indonesia's data protection is expected to improve once its draft Data Protection Law is established (expected date of approval unknown.)

Japan [10/1st]
Top-scorer Japan has been a global leader in establishing strong data protection laws and partnerships throughout the world.

Laos [0.8/28th]
While there is no data protection law, there are other laws such as the Law on Resistance and Prevention of Cybercrime, the Electronic Data Protection Law, and the Law on Electronic Transactions, which provide some form of data protection safeguards.

Malaysia [8.3/=10th]
One of the leading ASEAN states with a strong data protection law, and well-established data protection agency.

Mexico [9.2/=4th]
Mexico's data protection scores are perfect, save for its participation in the APEC CBPR, and seeking EU GDPR adequacy.

Myanmar [0.3/30th]
Myanmar does not have any data protection law, although there is a Law Protecting the Privacy and Security of Citizens (2017).

New Zealand [8.3/=10th]
One of the earliest economies to achieve an EU GDPR adequacy decision, New Zealand is one of the leader economies in developing strong data protection laws in Asia Pacific.

Peru [8.3/=10th]
Peru's data protection scores are perfect, save for its participation in the APEC CBPR, and seeking EU GDPR adequacy.

Philippines [7.8/=21st]
One of the leading ASEAN states with a strong data protection law, and well-established data protection agency.

Russia [8.3/=10th]
The Russian Federal Law on Personal Data (No. 152-FZ, 27 Jun 2006), is the backbone of Russian privacy laws, supported by Roskomnadzor, the federal authority in charge.

Singapore [9.2/=4th]
The top-scoring ASEAN state in the DPI 2020, with a strong data protection law, and well-established data protection agency.

South Africa [8.3/=10th]
The leading data protection economy on the African continent, South Africa boasts an established data protection act and regulator.

South Korea [9.4/2nd]
A pending EU GDPR adequacy application is the only thing stopping South Korea from joining Japan as a top-scoring data protection market.

Taiwan [8.3/=10th]
A strong Asian market with an established data protection law.

Thailand [8.3/=10th]
A leading ASEAN states with a freshly established data protection law in 2019.

United Arab Emirates [8.3/=10th]
Due to its establishment as a group of seven emirates (Abu Dhabi, Dubai, Ajman, Sharjah, Ras al Khaimah, Fujairah, and Umm al-Quwain), the UAE does not have a single data protection law for its market group. However, if the Dubai Data Protection Law (DIFC Law No. 1 of 2007) is any indication, the UAE has strong principles behind any data protection law other emirates may draw up.

United Kingdom [9.2/=4th]
As it (used to be) a member of the EU, the UK's data protection laws align with the EU GDPR. It remains to be seen if its strong data protection regime will continue post-Brexit.

United States [9.2/3rd]
The USA is an anomaly in the rankings as it does not have a national law for protecting data privacy. While we have used the EU-USA Privacy Shield Framework as an assessment benchmark, it would be prudent to note that this arrangement does not cover all US citizen data.

Vietnam [2.2/26th]
No data protection law exists, although some provisions for its aspects may be found in its cybersecurity law.

Appendix A: DPI 2020 Assessment Questions (with grading rubric)

Q1 Does the economy have a personal data protection law?
☐ Yes – 6
☐ No, but in draft form – 4
☐ No, but some principles are established in policies and guidelines or other laws (e.g. Constitution, Cybersecurity etc) – 2
☐ No - 0

Q2 Does the economy have a privacy enforcement authority (PEA)?
☐ Yes, a national PEA – 6
☐ No, but has sectoral regulator which enforces privacy (amongst other regulatory requirements) within the industrial sector – 2
☐ No – 0

Q3 [ASEAN Principle 1. Consent, Notification and Purpose] Does the personal data protection law require that organisations obtain consent from individuals, and notify them of the purposes of collection, use, and disclosure of their personal information by the organization?
☐ Yes in the PDP law and universal – 6
☐ Yes in the PDP law, in some cases – 4
☐ No, there is no PDP law, but this principle is protected or evident in other laws/sectoral regulations – 2
☐ No, there is no PDP law, and there are no protections around this principle – 0

Q4 [ASEAN Principle 1. Consent, Notification and Purpose] Does the personal data protection law have clear instructions on exemption circumstances by which consent from individuals for the collection, use, and disclosure of their personal information, is NOT required? E.g. where collection of personal information is authorised or required under domestic laws and regulations?
☐ Yes in the PDP law and universal – 6
☐ Yes in the PDP law, in some cases – 4
☐ No, there is no PDP law, but this principle is protected or evident in other laws/sectoral regulations – 2
☐ No, there is no PDP law, and there are no protections around this principle – 0

Q5 [ASEAN Principle 2. Accuracy of Personal Data] Does the personal data protection law require organisations to ensure that personal data be accurate and complete for the extent necessary for the purpose(s) for which the personal data is to be used or disclosed?
☐ Yes in the PDP law and universal – 6
☐ Yes in the PDP law, in some cases – 4
☐ No, there is no PDP law, but this principle is protected or evident in other laws/sectoral regulations – 2
☐ No, there is no PDP law, and there are no protections around this principle – 0

Q6 [ASEAN Principle 3. Security Safeguards] Does the personal data protection law require that personal data be appropriately protected against loss and unauthorised access, collection, use, disclosure, copying, modification, destruction or similar risks?
☐ Yes in the PDP law and universal – 6
☐ Yes in the PDP law, in some cases – 4
☐ No, there is no PDP law, but this principle is protected or evident in other laws/sectoral regulations – 2
☐ No, there is no PDP law, and there are no protections around this principle – 0

Q7 [ASEAN Principle 4. Access and Correction] Does the personal data protection law require organisations to, upon request from individuals, provide the individual access to his/her personal data which is in the possession or under the control of the organisation within a reasonable period of time, and correct an error or omission in his personal data, unless domestic laws and regulations require or authorise the organisation not to provide access or correct the personal data in the particular circumstances?
☐ Yes in the PDP law and universal – 6
☐ Yes in the PDP law, in some cases – 4
☐ No, there is no PDP law, but this principle is protected or evident in other laws/sectoral regulations – 2
☐ No, there is no PDP law, and there are no protections around this principle – 0

Q8 [ASEAN Principle 5. Transfers to Another Country or Territory] Does the law require that, before transferring personal data to another country or territory, the organisation should obtain the consent of the individual for the overseas transfer?

☐ Yes in the PDP law and universal – 6
☐ Yes in the PDP law, in some cases – 4
☐ No, there is no PDP law, but this principle is protected or evident in other laws/sectoral regulations – 2
☐ No, there is no PDP law, and there are no protections around this principle – 0

Q9 [ASEAN Principle 6. Retention] Does the personal data protection law require that an organisation cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes, or after a certain period of time (e.g. 5 yrs)?

☐ Yes in the PDP law and universal – 6
☐ Yes in the PDP law, in some cases – 4
☐ No, there is no PDP law, but this principle is protected or evident in other laws/sectoral regulations – 2
☐ No, there is no PDP law, and there are no protections around this principle – 0

Q10 [ASEAN Principle 7. Accountability] Does the personal data protection law require an organisation to, on request, provide clear and easily accessible information, such as how to contact the organisation, about its data protection policies and practices with respect to personal data in its possession or under its control?

☐ Yes in the PDP law and universal – 6
☐ Yes in the PDP law, in some cases – 4
☐ No, there is no PDP law, but this principle is protected or evident in other laws/sectoral regulations – 2
☐ No, there is no PDP law, and there are no protections around this principle – 0

Q11 Is the economy a participant of the EU's GDPR regime, or meets GDPR adequacy requirements?

☐ Yes – 6
☐ No, but has adequacy agreement – 4
☐ No, but is in talks for adequacy decision – 2
☐ No - 0

Q12 Is the economy a participant of the APEC CBPR or similar regional system (promoting an accountability rather than an adequacy system?

☐ Yes – 6
☐ No, but has applied – 2
☐ No - 0

Appendix B: Data Protection Assessments and Indexes

DLA Piper runs a data protection laws of the world database,[18] tracking each country against evidence of good data protection governance. It tracks aspects of strong data protection regulations, such as presence of a data protection law, how it is defined, its authorities, how the country manages registration and data protection officers, how the country has implemented rules around the collection and processing of data, transfer of data, data security, breach notification, enforcement mechanisms, rules around electronic marketing, and protections for online privacy.

Forrester has a **Global Heat Map of Privacy and Data Protection**,[19] which bands countries according to specific parameters, such as: privacy and data protection by country, scope of protection, covered entities, data transfers to other countries, EU adequacy, data protection established, government surveillance, privacy rights established in constitution.

France's Commission Nationale de l'Informatique et des Libertés (CNIL) has published a heatmap on data protection around the world,[20] showing where countries are an EU member country, and where other non-EU states are (1) adequate to the GDPR, (2) partially adequate, (3) where there are presence of a data protection authority and law(s), (4) where there are data protection law(s), and (5) where there is no specific data protection law. The CNIL's methodology therefore places countries in specific bands, with the strongest countries being EU member economies, and/or countries which are deemed GDPR adequate countries.

BestVPN also has a Privacy Index[21] which scores countries on how strong they are in protecting consumer privacy. It uses a composite score of seven factors to derive its scoresheet: (1) press freedom, (2) existence of data privacy laws, (3) democracy index, (4) freedom of opinion and expression is effectively guaranteed, (5) freedom from arbitrary interference with privacy is effectively guaranteed, (6) the government does not expropriate without lawful process and adequate compensation, and (7) cybercrime legislation worldwide.

Comparitech has a similar Surveillance States Index,[22] which ranked 47 countries by privacy laws and government surveillance indicators, including: constitutional and statutory protection, enforcement, identity cards and biometrics, data sharing, video surveillance, communication interception, workplace monitoring, government access to data, communications data retention, surveillance of movement for finance and medical data, border issues, leadership, and democratic safeguards.

[18] https://www.dlapiperdataprotection.com/
[19] https://heatmap.forrestertools.com/
[20] https://www.cnil.fr/en/data-protection-around-the-world
[21] https://bestvpn.org/privacy-index/
[22] https://www.comparitech.com/blog/vpn-privacy/surveillance-states/

Appendix C: International/Regional Data Protection Frameworks and Mechanisms

European Union's (EU) General Data Protection Regulation (GDPR) 2018

The **EU GDPR**[23] came into effect on 25 May 2018, and was established as a legally-enforceable legislation in all 28 EU economies: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.[24]

The GDPR centres around the individual's rights,[25] which include:

1. Right to know about when personal information is collected – to have transparency on information about the processing of their personal data;
2. Right of access – to obtain access to the personal data held about them;
3. Right to rectification – to ask for incorrect, inaccurate or incomplete personal data to be corrected;
4. Right to erasure/be forgotten - request that personal data be erased when it is no longer needed or if processing it is unlawful;
5. to object to the processing of their personal data for marketing purposes or on grounds relating to their particular situation;
6. Right to data portability – to receive their personal data in a machine-readable format and send it to another controller;
7. Right to object and automated individual decision-making – to request the restriction of the processing of their personal data in specific cases; and/or to request that decisions based on automated processing concerning them or significantly affecting them and based on their personal data are made by natural persons, not only by computers. They also have the right in this case to express their point of view and to contest the decision.

The GDPR is an adequacy-based regime, and non-EU countries may apply for the European Commission (EC) to determine if it offers an adequate level of data protection. A successful adequacy decision means that personal data can be transmitted to that country from the EU (and Norway, Liechtenstein and Iceland) without further safeguards.

To date, the EC has recognized the following markets as providing adequate protection: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, the United States of America (limited to the Privacy Shield framework), with South Korea having an ongoing application.

APEC Cross-Border Privacy Rules (CBPR) System

Another data protection framework which has developed is the **APEC CBPR System,**[26] which was built on the APEC Privacy Framework 2005, updated in 2015, which in turn was derived from the Organisation for Economic Co-operation and Development (OECD) eight Privacy Principles, developed in 1980 and updated in 2013.[27]

The APEC CBPR system was endorsed by APEC leaders in 2011, and involves nine Information Privacy Principles to prevent abuse and misuse of information: (1) preventing harm, (2) notice, (3) collection limitation, (4) uses of personal information, (5) choice, (6) integrity of personal information, (7) security safeguards, (8) access and correction, and (9) accountability.

However, unlike the EU GDPR where compliance is mandatory and applies to all EU economies, the APEC CBPR is a voluntary, accountability-based system designed for the private sector to gain a trusted accreditation proving that their business practices adhered to specific privacy rules.

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679
[24] The United Kingdom has officially left the EU as of 12 April 2019; negotiations are ongoing regarding the technical aspects of its withdrawal.
[25] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en
[26] http://cbprs.org/about-cbprs/
[27] https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

About the TRPC Data Protection Index 2020 (DPI 2020)

The inaugural DPI 2020 is the first index to establish an objective, data protection assessment mechanism based on the seven Principles of Personal Data Protection in the ASEAN Framework on Personal Data Protection 2016. It scores 30 markets across 12 questions that assess an economy's data protection laws and regulatory environment. To enable policymakers to conduct comparisons on a national and international level, this first iteration of the DPI includes all economies represented in ASEAN (10 member states), APEC (21 member economies), and the G20 (20 member economies).

About TRPC Pte Ltd

TRPC is a boutique consulting and research firm with over 25 years' experience in the telecommunications and ICT industries in the Asia-Pacific. We offer specialised advisory, research, and training services, with a focus on regulatory and strategic business issues, and possess an extensive network of industry experts and professionals throughout the region.

Our research focuses on the economic impact of the emergence of new business models and the developments in telecommunications and information technologies, as well as their associated policy and regulatory issues. Our expertise encompasses both the more developed ICT countries (e.g. South Korea, Japan, and Hong Kong) and those with fast-growing and emerging ICT industries (e.g. Indonesia, Philippines, and Vietnam).

We provide an intersection between academia, businesses, and relevant policy makers for the technology, telecommunications, and the ICT industries broadly defined, including the impact upon, and opportunities generated by, the use of new digital technologies in non-tech industries. Our recent work covers a range of up-and-coming areas such as blockchain and cryptocurrencies, digital identities, cloud computing and healthcare, cross-border data flows, and data analytics and credit ratings systems, among others.

TRPC has offices in Hong Kong, Melbourne, and Singapore with on-the-ground presence or associates throughout the Asia-Pacific region. Visit us online at https://trpc.biz or contact us at info@trpc.biz.