Privacy and data protection laws of Bali Process member States
The Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime (the Bali Process) was established in 2002 and is a voluntary and non-binding regional consultative process co-chaired by the Governments of Australia and Indonesia and comprising over 45 member countries and organizations.

Queries about this research report should be addressed to the Regional Support Office (RSO) to the Bali Process at:

Email: info@rso.baliprocess.net RSO website: http://www.baliprocess.net/regional-support-office

Published May 2015.
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Table 1: Common Privacy Principles</td>
<td>8</td>
</tr>
<tr>
<td>Table 2: Privacy laws of Bali Process member States</td>
<td>10</td>
</tr>
<tr>
<td>Introduction</td>
<td>16</td>
</tr>
<tr>
<td>Afghanistan</td>
<td>21</td>
</tr>
<tr>
<td>Australia</td>
<td>22</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>26</td>
</tr>
<tr>
<td>Bhutan</td>
<td>27</td>
</tr>
<tr>
<td>Brunei Darussalam</td>
<td>27</td>
</tr>
<tr>
<td>Cambodia</td>
<td>27</td>
</tr>
<tr>
<td>China</td>
<td>28</td>
</tr>
<tr>
<td>Democratic People’s Republic of Korea</td>
<td>29</td>
</tr>
<tr>
<td>Fiji</td>
<td>29</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>30</td>
</tr>
<tr>
<td>India</td>
<td>34</td>
</tr>
<tr>
<td>Indonesia</td>
<td>36</td>
</tr>
<tr>
<td>Iran</td>
<td>38</td>
</tr>
<tr>
<td>Iraq</td>
<td>38</td>
</tr>
<tr>
<td>Iraq</td>
<td>39</td>
</tr>
<tr>
<td>Japan</td>
<td>44</td>
</tr>
<tr>
<td>Jordan</td>
<td>45</td>
</tr>
<tr>
<td>Kiribati</td>
<td>45</td>
</tr>
<tr>
<td>Lao People’s Democratic Republic</td>
<td>45</td>
</tr>
<tr>
<td>Macao</td>
<td>46</td>
</tr>
<tr>
<td>Malaysia</td>
<td>50</td>
</tr>
<tr>
<td>Maldives</td>
<td>50</td>
</tr>
<tr>
<td>Mongolia</td>
<td>51</td>
</tr>
<tr>
<td>Myanmar</td>
<td>52</td>
</tr>
</tbody>
</table>
Privacy is recognized as a fundamental human right and is emerging as one of the most prominent issues for the Asia-Pacific region. The collection, use and disclosure of personal information by governments is expanding exponentially throughout the region, including within the areas of migration and law enforcement in the context of irregular migration, people smuggling, trafficking in persons and related transnational crime.

Addressing transnational challenges requires regional and international cooperation that increasingly involves the exchange of personal information. The exchange of personal information between governments can be useful in trends reporting, intelligence sharing, detecting, investigating and prosecuting transnational crimes, verifying identities of travelers, migrants and asylum seekers, resettlement and assisted voluntary returns, and reissuing of lost and stolen travel documents.

The exchange of personal information for these purposes has implications on the individuals concerned. The public policy benefits of exchanging personal information must be balanced against the individual’s right to privacy. The significance of this balancing exercise is reflected in the Regional Cooperation Framework of the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crimes. Under the Regional Cooperation Framework, member States are encouraged to enter into practical arrangements to address irregular migration, people smuggling, human trafficking and related transnational crime which, among other things, “support and promote increased information exchange, while respecting confidentiality and upholding the privacy of affected persons.” Member States are encouraged to not only consider the privacy protections available within their own jurisdiction, but also consider the level of privacy protection available within the laws of partnering jurisdictions if they are to cooperate with each other through exchanging personal information.

The Regional Support Office of the Bali Process (RSO), in order to facilitate the operationalization of the Regional Cooperation Framework, conducted desk-based research on the privacy laws of Bali Process member States to support the development of information exchange frameworks and arrangements between Bali Process members. The key findings from the research outlined below summarize the main features and emerging trends of privacy protection among the Bali Process membership. This research may assist member States in developing information exchange frameworks and arrangements which include privacy safeguards that are consistent with international privacy standards and principles and with domestic laws.

This research can also be useful for any context in which information is exchanged between governments, assisting both member States and individuals in understanding how personal information is and can be protected, both domestically and during cross-border transfers of personal information. It may act as a useful guide for understanding the overall landscape of privacy protection in the Asia-Pacific region, and in particular which privacy laws apply to government agencies. It highlights the key emerging trends that can assist States in developing their own laws that are harmonized and consistent with regional and international standards.
Key Findings

1. There is a broad and consistent recognition of the general right to privacy among Bali Process member States. The constitutions of almost all Bali Process member States contain recognition of either the right to privacy or rights relating to privacy. Such rights can be guaranteed in different ways. For example, some national constitutions explicitly guarantee a right to privacy. Other national constitutions implicitly guarantee privacy through the right to personal dignity, the right to private communications, and the freedom of interference with the private home and correspondence. The courts of some jurisdictions have implied the right to privacy within these privacy-related rights.

Supplementing national constitutions are the domestic laws of Bali Process member States relating to privacy and data protection. While domestic laws may be diverse and varying (see Key Finding 2), they have not been developed in a vacuum. In addition to national constitutions, they have been broadly drawn from international privacy standards and principles, which include:

- the general right to privacy enshrined in international human rights instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights; and

- common international privacy principles outlined in international privacy frameworks such as the OECD Guidelines governing the Protection of Privacy and Transborder Flows, the UN Guidelines for the Regulation of Computerized Personal Data Files, the EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data and the APEC Privacy Framework. The common privacy principles are broadly summarized in Table One at the end of this Executive Summary, noting that there are both substantial and nuanced differences between how these features and principles are expressed by these four international privacy frameworks.

2. There are diverse types of laws and varying levels of privacy and data protection among Bali Process member States. Within the broad recognition of the general right to privacy, varying levels of privacy and data protection arise from a diverse type of domestic laws within the membership. Privacy and data protection is, depending upon each jurisdiction, found in comprehensive privacy legislation, right to information legislation, public administration legislation, civil codes, electronic commerce and transaction legislation, or information technology legislation. Table Two at the end of this Executive Summary provides an overview of the privacy laws of all Bali Process member States.

3. Nine Bali Process member States have comprehensive and consolidated privacy laws that apply to government agencies. These privacy laws are broadly consistent with all or most of the common international privacy principles, which include requirements relating to limitations on the collection, use and disclosure of personal information, informed consent, notification and purpose specification, data quality, access and correction, data retention, data security, and accountability mechanisms. While these laws are comprehensive and provide a substantial level of privacy and data protection, there exist a broad range of exemptions applicable to government agencies (see Key Finding 5 below).
4. Of the States without comprehensive privacy laws applying to the government agencies, 16 Bali Process member States have laws which contain a moderate level of privacy protection.

Some States have comprehensive privacy laws that have no or limited application to government agencies or have limited territorial application within the State. Some States have privacy protections within civil codes, which protect against infringements upon an individual’s privacy.

Some States have electronic commerce and transactions legislation or information technology legislation that provides a moderate level of privacy protection to electronic information. Where these laws apply to government agencies, the privacy protections may have practical application that is broad, if not necessarily complete. This is because a growing proportion of information held by government agencies is now electronic.

Many States have right to information, access to information or freedom of information legislation, which provides two forms of privacy protection. These types of legislation would ordinarily provide the right to access and, in most cases but not all, the right to correct personal information held by government agencies. Right to information legislation may also provide restrictions on the disclosure of personal information where it infringes on an individual’s privacy.

5. There are clear categories of exemptions and exceptions available to government agencies provided under privacy laws. All privacy laws applicable to government agencies provide a broad range of exemptions and exceptions, in recognition of the need to balance between protecting privacy and protecting national sovereignty, national security, public safety and other public interests. In some jurisdictions, law enforcement and national security agencies are exempt generally from the application of privacy laws. In other jurisdictions, while privacy laws apply to government agencies, exceptions to certain requirements apply to certain actions of government agencies. Most relevantly, exceptions generally relate to actions required or authorized under the law or court order, and actions undertaken for law enforcement purposes. These exceptions give government agencies broad scope to use and exchange personal information if there are laws authorizing the exchange or if it is done for a law enforcement purpose. These exemptions and exceptions are provided for the purposes of legitimate public interests and while they are relatively broad, they nevertheless provide privacy protective limits on the exercise of government power.

In relation to limitations on the collection, use and disclosure of personal information, the common broad types of exceptions available relate to:

- prevention or detection of crime, unlawful or seriously improper conduct;
- safeguarding national security, defence or international relations;
- a serious threat to life and body of a person, or public health or security;
- requirements or authorization by a law or court order;
- being reasonably necessary for the performance of agency functions prescribed in law or regulation, including enforcement related activities;
- authorization by a privacy authority or other authority;
- prescribed "permitted general situations" declared under certain privacy legislation, which relevantly include law enforcement activities;
- compliance with a legal obligation to which the data controller is subject; and
- fulfilment of legitimate interests of data controller, except where that is overridden by interests for fundamental rights, freedoms and guarantees of data subject.
In relation to access and correction rights, the common broad categories for exemptions and exceptions relate to disclosure that:

- violates the privacy of another individual, unless disclosure is approved by a law or court;
- is an offence under domestic laws;
- is expressly forbidden by any court or tribunal or which may constitute contempt of court;
- harms or results in danger to the national security, national interest, public safety, or political, economic and social relations with other governments;
- reveals information that is secret or received in confidence from a foreign government;
- disrupts the process of detection, investigation and prosecution of criminal offences; and
- reveals information given in confidence to any law enforcement agency.

6. Many jurisdictions are continuing to update, develop or introduce privacy laws to meet the evolving needs of their domestic context. In particular, countries are developing privacy laws as part of government initiatives in relation to e-government initiatives, national identification card projects, right to government information reforms, and border management programs.

7. An emerging trend is specific protection relating to cross-border transfers of personal information. In jurisdictions where specific protection applies, cross-border transfers of personal information are permitted where the individual has specifically consented to the transfer. Otherwise, cross-border transfers are generally permitted where the recipient place or jurisdiction has an “adequate” or “substantially similar” level of protection as provided under the relevant privacy law. Assessing the level of protection in many cases is determined by the relevant privacy authority, but under some laws it may be up to the data controller or data user if there are reasonable grounds for believing that there is an adequate level of protection. The common exceptions from these requirements relevantly include where:

- the transfer is authorized by legislation or required under any convention, international agreement or instrument;
- a privacy authority has made a determination to permit the specific transfer;
- data controllers have adduced sufficiently adequate safeguards specific to the transfer, for example through contractual arrangements that result in a similar level of protection;
- the transfer is for the purposes of prevention, investigation and prosecution of criminal offences;
- a prescribed “general permitted situation” exists, including where both the disclosing agency and the recipient agency are enforcement agencies;
- the transfer is necessary for the protection of individual’s life, protection of the public interest, exercise or defence of a legal right or obligation; and
- the transfer is for the avoidance or mitigation of adverse action against the data subject, and it is not practicable to obtain the written consent of the data subject, and if it was practicable, the data subject would have provided consent.
8. Another emerging trend is specific protections relating to the automatic matching of personal information. The specific protections relating to automatic matching of personal information, whether by one government agency or between government agencies, are generally threefold. Firstly, automatic matching must undergo an approval process. Approvals are generally based on authorization from legislation or notification and approval from the relevant privacy authority. In some jurisdictions, the consent of the individual also amounts to approval. In some jurisdictions, where information from automatic matching programs is exchanged between agencies, written agreements governing the exchange need to be entered into and approved by the relevant privacy authority. Secondly, any adverse action taken against an individual as a result of automatic matching must be notified to the individual concerned, and a minimum response period must be provided to the individual before adverse action is taken. However, consistent with the general exceptions outlined above in Key Finding 5, broad exceptions to the requirement of notification are available to government agencies. Thirdly, general oversight protections apply, requiring agency reporting to the relevant privacy authority, and periodical reporting and review by the relevant privacy authority.
## Table 1: Common Privacy Principles

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection</strong> – personal information should only be collected by lawful and fair means, and where appropriate, with the knowledge or consent of the data subject.</td>
<td>Collection Limitation Principle</td>
<td>Principle of lawfulness and fairness</td>
<td>Collection Limitation and Notice Principles</td>
<td>Section IV (“Information to be given to the data subject”)</td>
</tr>
<tr>
<td><strong>Purpose</strong> – the purpose of data collection should be notified to the individual before or at the time of the collection. Subsequent use should be limited to the specified purpose or compatible purposes.</td>
<td>Purpose Specification Principle</td>
<td>Principle of the purpose-specification</td>
<td>Notice Principle</td>
<td>Section I (“Principles relating to Data Quality”)</td>
</tr>
<tr>
<td><strong>Use</strong> – personal information should only be used for the purpose that it was collected, unless otherwise consented to by the individual or by authority of the law.</td>
<td>Use Limitation Principle</td>
<td>Principle of the purpose-specification</td>
<td>Uses of Personal Information Principle</td>
<td>Section II (“Criteria for making data processing legitimate”)</td>
</tr>
<tr>
<td><strong>Data Quality</strong> – personal information should be relevant to the purposes for which they are used, and be complete, accurate and up-to-date.</td>
<td>Data Quality Principle</td>
<td>Principle of accuracy</td>
<td>Integrity of Personal Information Principle</td>
<td>Section I (“Principles relating to Data Quality”)</td>
</tr>
<tr>
<td><strong>Individual participation</strong> – individuals should be able to access, amend and correct the personal information held about them.</td>
<td>Individual Participation Principle</td>
<td>Principle of interested-person access</td>
<td>Access and Correction Principle</td>
<td>Section V (“Data subject’s right of access to data”)</td>
</tr>
<tr>
<td><strong>Security Safeguards</strong> – safeguards should be established to ensure the security of personal information against loss or unauthorized access, destruction, use, modification or disclosure.</td>
<td>Security Safeguards Principle</td>
<td>Principle of security</td>
<td>Security Safeguards Principle</td>
<td>Section VII (“Data subjects right to object”)</td>
</tr>
<tr>
<td><strong>Accountability</strong> – data controllers should be held accountable for adherence to privacy principles.</td>
<td>Accountability Principle</td>
<td>Supervision and sanctions (Article 8)</td>
<td>Accountability Principle</td>
<td>Section VIII (“Confidentiality and security of processing”)</td>
</tr>
<tr>
<td><strong>Cross-border transfer of personal information</strong> – substantial or sufficient safeguards must exist in recipient jurisdiction to ensure continuing level of protection consistent with privacy principles.</td>
<td>Basic Principles of International Application</td>
<td>Transborder data flows (Article 9)</td>
<td>Voluntary Cross Border Privacy Rules</td>
<td>Chapter IV (“Transfer of personal data to third countries”)</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>----------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Openness</strong> – information about privacy frameworks should generally be open to</td>
<td>Openness Principle</td>
<td>-</td>
<td>-</td>
<td>Article 21 (“Publicizing of processing operations”)</td>
</tr>
<tr>
<td>the public.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Prevention of harm and misuse of personal information</strong> – protection should be</td>
<td>-</td>
<td>-</td>
<td>Preventing Harm</td>
<td></td>
</tr>
<tr>
<td>designed to prevent the misuse of personal information, and remedial measures</td>
<td></td>
<td></td>
<td>Principle</td>
<td></td>
</tr>
<tr>
<td>should be proportionate to the likelihood and severity of any harm caused.</td>
<td></td>
<td></td>
<td>of non-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>discrimination</td>
<td></td>
</tr>
<tr>
<td><strong>No unfair-discrimination against data subjects</strong> – data likely to give rise to</td>
<td>Article 19</td>
<td>Principle of</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>unlawful or arbitrary discrimination should not be compiled.</td>
<td></td>
<td>the purpose-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>specification</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Retention</strong> – personal information should only be retained for the period</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Section 1 (“Principles relating to data quality”)</td>
</tr>
<tr>
<td>necessary to achieve the specified purpose.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Choice</strong> – individuals should be provided with clear, prominent, easily</td>
<td>-</td>
<td>-</td>
<td>Choice Principle</td>
<td>Article 14 (“Data subject’s right to object”)</td>
</tr>
<tr>
<td>understandable, accessible, and affordable mechanisms to exercise choice in</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>relation to collection, use and disclosure of personal information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 2: Privacy laws of Bali Process member States

<table>
<thead>
<tr>
<th>Country</th>
<th>Privacy law</th>
<th>Application to government agencies</th>
<th>Cross-border transfers</th>
<th>Key features of privacy law</th>
<th>Privacy authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>Constitutional right Access to Information Law 2014</td>
<td>Yes, with a wide range of exceptions</td>
<td>Yes, with a wide range of exceptions</td>
<td>Access, use and disclosure limitations, notification requirements, data quality, access and correction, data security, accountability</td>
<td>Access to Information Monitoring Commission</td>
</tr>
<tr>
<td>Australia</td>
<td>Privacy Act 1988 Freedom of Information Act 1992</td>
<td>Yes, with a wide range of exceptions</td>
<td>Substantially similar level of protection, with exceptions</td>
<td>Access to information</td>
<td>Australian Information Commissioner</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Constitutional right Right to Information Act 2009</td>
<td>Yes, with a wide range of exceptions</td>
<td>-</td>
<td>General protection of secrecy of electronic information, civil actions against invasion of privacy, access and correction</td>
<td>-</td>
</tr>
<tr>
<td>Bhutan</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Brunei</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Cambodia</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>China</td>
<td>Constitutional right Various laws</td>
<td>Yes, with a wide range of exceptions</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Democratic People’s Republic of Korea</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Country</td>
<td>Privacy law</td>
<td>Application to government agencies</td>
<td>Key features of privacy law</td>
<td>Cross-border transfers</td>
<td>Automatic matching</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Fiji</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention, data security, accountability</td>
<td>-</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Basic Law right Personal Data (Privacy) Ordinance 1996</td>
<td>Yes, with a wide range of exceptions</td>
<td>-</td>
<td>Similar level of protection, with exceptions</td>
<td>Approval required; adverse action requirements</td>
</tr>
<tr>
<td>India</td>
<td>Constitutional right Information Technology Act 2000 Right to Information Act 2005</td>
<td>No (ITA), with a wide range of exceptions</td>
<td>Access and correction</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Constitutional right Various laws</td>
<td>Yes, with a wide range of exceptions</td>
<td>Limitations on collection, use and disclosure, data security, data quality, access to information</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Iran</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Iraq</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Japan</td>
<td>Constitutional right Act on Protection of Personal Information Held by Administrative Organs 2003 Law Concerning Access to Information Held by Administrative Organs 1996</td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention, data security, accountability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Country</td>
<td>Privacy law</td>
<td>Application to government agencies</td>
<td>Key features of privacy law</td>
<td>Cross-border transfers</td>
<td>Automatic matching</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------</td>
<td>------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Jordan</td>
<td>Constitutional right Law on Securing the Right to Information Access 2007</td>
<td>Yes, with a wide range of exceptions</td>
<td>Access to information</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Kiribati</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Lao People's Democratic Republic</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Macao</td>
<td>Basic Law right Personal Data Protection Act 2005</td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention, data security, accountability</td>
<td>Adequate level of protection, with exceptions</td>
<td>Approval required; adverse action requirements</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Constitutional right Personal Data Protection Act 2010</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Maldives</td>
<td>Constitutional right Right to Information Act 2014</td>
<td>Yes, with a wide range of exceptions</td>
<td>Access and correction</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Mongolia</td>
<td>Constitutional right Law on Information Transparency &amp; Right to Information 2011</td>
<td>Yes, with a wide range of exceptions</td>
<td>Access to information</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Myanmar</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Country</td>
<td>Privacy law</td>
<td>Application to government agencies</td>
<td>Key features of privacy law</td>
<td>Cross-border transfers</td>
<td>Automatic matching</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Nauru</td>
<td>Constitutional right</td>
<td>-</td>
<td>Access and correction, limitation on use and disclosure</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Nepal</td>
<td>Constitutional right</td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention, data security, accountability</td>
<td>Adequate level of protection, with exceptions</td>
<td>Approval required for automated processing</td>
</tr>
<tr>
<td>New Caledonia</td>
<td>Data Protection Act 1978 (French)</td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention, data security, accountability</td>
<td>Adequate level of protection, with exceptions</td>
<td>Approval required for automated processing</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Privacy Act 1993</td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention, data security, accountability</td>
<td>Adequate level of protection, with exceptions</td>
<td>Approval required for programs and agreements; adverse action requirements</td>
</tr>
<tr>
<td>Pakistan</td>
<td>Constitutional right</td>
<td>Yes, with a wide range of exceptions</td>
<td>Access and correction</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Palau</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Papua New Guinea</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Country</td>
<td>Privacy law</td>
<td>Application to government agencies</td>
<td>Key features of privacy law</td>
<td>Cross-border transfers</td>
<td>Automatic matching</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>The Philippines</td>
<td>Constitutional right <em>Data Protection Act 2007</em></td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention, data security, accountability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>Constitutional right <em>Personal Information Protection Act 2011</em> <em>Act on Disclosure of Information by Public Agencies 1996</em></td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention, data security, accountability</td>
<td>Adequate data protection, with exceptions</td>
<td>-</td>
</tr>
<tr>
<td>Samoa</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Singapore</td>
<td><em>Personal Data Protection Act 2012</em></td>
<td>Yes, with a wide range of exceptions</td>
<td>Data quality, access and correction, data retention, data security</td>
<td>Adequate level of protection, with exceptions</td>
<td>-</td>
</tr>
<tr>
<td>Solomon Islands</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Syria</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Thailand</td>
<td>Constitutional right <em>Official Information Act 1997</em></td>
<td>Yes, with a wide range of exceptions</td>
<td>Disclosure limitations, notification, data security, access and correction</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Country</td>
<td>Privacy law</td>
<td>Application to government agencies</td>
<td>Key features of privacy law</td>
<td>Cross-border transfers</td>
<td>Automatic matching</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Timor-Leste</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Tonga</td>
<td>Constitutional right</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Turkey</td>
<td>Constitutional right Various laws</td>
<td>Yes, with a wide range of exceptions</td>
<td>Access to information, protection against violation of personal rights</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>Constitutional right Data Protection Law of 2007 (Dubai only)</td>
<td>Yes, with a wide range of exceptions</td>
<td>Use and disclosure limitations, notification requirements, data security, data quality, access and correction, data retention</td>
<td>Adequate level of protection, with exceptions</td>
<td>-</td>
</tr>
<tr>
<td>United States of America</td>
<td>Constitutional right Privacy Act 1974 Freedom of Information Act 1967</td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification requirements, data quality, access and correction, data retention</td>
<td>-</td>
<td>Approval required for programs and agreements; adverse action requirements</td>
</tr>
<tr>
<td>Vanuatu</td>
<td>Constitutional right Electronic Transactions Act 2000</td>
<td>-</td>
<td>Regulations relating to standards for processing personal data have yet to be made.</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Viet Nam</td>
<td>Civil Code right Law on Information Technology 2006</td>
<td>Yes, with a wide range of exceptions</td>
<td>Collection, use and disclosure limitations, notification, access and correction, data retention</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Introduction

Background

Privacy is recognized as a fundamental human right and is emerging as one of the most prominent issues for the Asia-Pacific region. The collection, use and disclosure of personal information are expanding exponentially throughout the region and across a wide range of areas. Personal information is increasingly flowing within the private sectors in relation to social media, electronic commerce and finance, consumer products, and international data processing centers, and within the public sector in relation to social security, national identity systems, international migration, early detection, investigation and prosecution of migration offences, and protection of refugees.

Within the context of the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime, member States are increasingly collecting information about individuals as part of their domestic border management, law enforcement, and protection practices. This includes collection of personal information, including biometric information, for purposes of national identification, issuing passports, border and migration management, visa processing, and refugee assessments.

The exchange of personal information is also becoming more common, particularly within the context of irregular migration, people smuggling, trafficking in persons and related transnational crime. Addressing transnational challenges requires regional and international cooperation that increasingly includes the exchange of personal information between governments. Exchanges of personal information can be useful in trends reporting, intelligence sharing, assisting in the detection, investigation and prosecution of transnational crimes, verifying identities of travelers, migrants and asylum seekers, resettlement and assisted voluntary returns, and reissuing of lost and stolen travel documents.

The exchange of personal information for these purposes has implications on the individuals concerned. The public policy benefits of these activities must be balanced against the individual’s right to privacy. The significance of this balancing exercise is reflected in the Regional Cooperation Framework of the Bali Process, which encourages member States to enter into practical arrangements to address irregular migration, people smuggling, human trafficking and related transnational crime which “support and promote increased information exchange, while respecting confidentiality and upholding the privacy of affected persons.” 1 This means that member States are encouraged to not only consider the privacy protections within their own jurisdiction, but also consider the level of privacy protection of partnering jurisdictions if they are to collaborate with and exchange personal information to those receiving partnering jurisdictions.

The Regional Support Office of the Bali Process (RSO), in order to facilitate the operationalization of the Regional Cooperation Framework, has conducted research on the privacy laws within the Asia-Pacific region to support the development of information exchange frameworks and arrangements between Bali Process members. This research may assist member States in developing information exchange frameworks and arrangements which include privacy safeguards that are drawn from international privacy standards and principles, and are compatible with domestic laws of member States. This research can also be a useful guide for understanding the

---

overall landscape of privacy protection in the Asia-Pacific region, and in particular which privacy laws apply to government agencies. It highlights the key emerging trends that can assist States in developing their own laws in order to be harmonized and consistent with international and regional standards.

Comprehensive research reports have recently been produced on privacy laws within the region. However these publications are written mostly for a private sector audience. For example, much of this research has been published to advise companies about electronic transactions and establishing offshore data processing centers. There exists no report of privacy laws within the region focused solely on the applicability of privacy laws to government agencies, and in particular agencies, such as law enforcement and immigration agencies. These are the entities most relevant to addressing irregular migration, people smuggling, trafficking in persons and related transnational crime. This report aims to fill this gap.

**International standards relating to privacy**

The privacy laws of member States were developed within an international privacy framework and do not exist in isolation. The rights to personal liberty, privacy, and protection of home and correspondence contained in many members’ constitutions reflect fundamental human rights as enshrined in human rights instruments. Under the *Universal Declaration of Human Rights* (UDHR), Article 12 provides that:

> “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Under the *International Covenant on Civil and Political Rights* (ICCPR), Article 17 similarly provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.”

Under the *Convention on the Rights of the Child* (CRC), Article 16 similarly provides:

> 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation.
> 2. The child has the right to the protection of the law against such interference or attacks.”

Article 40(vii) of the CRC further provides that every child alleged or accused of having infringed a penal law is guaranteed “to have his or her privacy fully respected at all stages of the proceedings.”

Within the Bali Process context, relevant international treaties contain more specific privacy protections. Article 6 of the *United Nations Convention on Transnational Organized Crime* provides that:

> “In appropriate cases and to the extent possible under its domestic law, each State Party shall protect the privacy and identity of victims of trafficking in persons, including, inter alia, by making legal proceedings relating to such trafficking confidential.”

---

These broad expressions of the right to privacy have been broadened by standards and privacy principles outlined in international privacy frameworks, including the OECD Guidelines, UN Guidelines, the EU Data Protection Directive and the APEC Privacy Framework. While no single definitive instrument exists that creates a uniform international or regional privacy framework, the above privacy frameworks have many common features and principles. A comparison of these privacy frameworks is provided in Table One of the Executive Summary.

Another significant element of these principles is the acknowledgement that the right to privacy is not absolute. The general right to privacy may be balanced against other public interests, and exceptions and derogations are permitted in certain appropriate circumstances. For example, Principle 6 of the UN Guidelines provides countries with the discretion to create exceptions to:

“protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.”

Paragraph 4 of the OECD Guidelines states that:

“Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy (“ordre public”), should be:
   a) as few as possible, and
   b) made known to the public.”

Article 13 of the APEC Privacy Framework provides that:

“Exceptions to these Principles contained in Part III of this Framework, including those relating to national sovereignty, national security, public safety and public policy should be:
   a) limited and proportional to meeting the objectives to which the exceptions relate; and,
   b) (i) made known to the public; or,
      (ii) in accordance with law.”

Similarly, Article 13 of the EU Directive relevantly provides that:

“Member States may adopt legislative measures to restrict the scope of the obligations and rights … when such a restriction constitutes a necessary measure to safeguard:
   (a) national security;
   (b) defence;
   (c) public security;
   (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
   …
   (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
   (g) the protection of the data subject or of the rights and freedoms of others.”

The common features outlined above, namely the fundamental privacy and privacy related rights from human rights instruments, the privacy principles derived from international and regional privacy frameworks, and the balancing exercise between the general right to privacy and other public policy
interests, form the general international standards relating to privacy. It is within the context of these standards that domestic privacy laws have been developed.

**Methodology**

The RSO conducted this research to support information exchange frameworks and arrangements between interested members of the Bali Process. The research aimed to provide an analysis for the RSO and Bali Process members to enhance understanding of the privacy protections that arise in the laws of members of the Bali Process. For this reason, this research focused on the application of national privacy laws on national government or public sector agencies, and in particular, immigration and law enforcement agencies. This report does not provide descriptions of criminal laws or laws that apply only to the private sector or seek to provide a broad exemption to government agencies.

This research was conducted through desk research and analysis of publicly available laws. Wherever possible, official English language translations of national laws were analyzed, however unofficial English translations have been used for several laws. As part of the desk research, only the interpretation of the text and language of constitutions and laws have been recorded. There was no assessment of the implementation and enforcement of privacy laws in practice. This may be the basis for further, more targeted research that is outside the scope of this report.

**Terminology**

Given the broad and diverse legal contexts of the Bali Process membership, differences arise in terminology used within the privacy laws of Bali Process member States. Wherever possible, the terms used within this report reflect the domestic laws of the countries. Some laws may use terminology or language from the EU Directive, while others may draw from their own social, cultural and legal contexts. The differing terms, which generally refer to the same or similar concepts, used within privacy laws include:

- personal data, personal information, or retained personal information;
- individual, person, or data subject;
- data processing, use, utilization, or handling;
- disclosure, transfer, or provision;
- public body, public agency, public sector agency, administrative organ, entity; and
- data controller, personal information controller, electronic system operator, head of an administrative organ, data user, or data processor.
**Acronyms and Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APEC Privacy Framework</td>
<td>APEC Privacy Framework</td>
</tr>
<tr>
<td>Bali Process</td>
<td>Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime</td>
</tr>
<tr>
<td>CAT</td>
<td>Convention Against Torture, or Cruel, Inhumane or Degrading Treatment</td>
</tr>
<tr>
<td>CRC</td>
<td>Convention on the Rights of the Child</td>
</tr>
<tr>
<td>EU Directive</td>
<td>EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>IOM</td>
<td>International Organization for Migration</td>
</tr>
<tr>
<td>OECD Guidelines</td>
<td>OECD Guidelines governing the Protection of Privacy and Transborder Flows</td>
</tr>
<tr>
<td>RSO</td>
<td>Regional Support Office of the Bali Process</td>
</tr>
<tr>
<td>UDHR</td>
<td>Universal Declaration of Human Rights</td>
</tr>
<tr>
<td>UN Guidelines</td>
<td>UN Guidelines for the Regulation of Computerized Personal Data Files</td>
</tr>
<tr>
<td>UNHCR</td>
<td>United Nations High Commissioner for Refugees</td>
</tr>
<tr>
<td>UNTOC</td>
<td>United Nations Convention against Transnational Organized Crime</td>
</tr>
</tbody>
</table>
Afghanistan

The right to privacy is implicitly provided for in the Constitution of Afghanistan. Article 37 guarantees the right to confidentiality and freedom of correspondance. Article 38 guarantees protection from entering or inspection of a private residence without prior permission of the resident or holding a court order.

While there is no comprehensive law relating to privacy and data protection, there are some laws with provide some forms of privacy protection.

**Access to Information Law 2014**

The Access to Information Law 2014 provides individuals with the right to access to all information held by public authorities, subject to limited exceptions. Those exceptions relevantly include, under Article 15, where the disclosure of information held by public authorities:

- results in danger to the independence, sovereignty, territorial integrity, national security and national interest;
- harms Afghanistan's political, economic and social bonds with other countries;
- becomes a barrier in crime detection or crime prevention;
- disrupts the process of detection, investigation and prosecution of the suspect or the safeguards in this regard; or
- violates the privacy of an individual, unless a competent court approves disclosure of personal information, or the copyright law and competition support law and all other legislative documents are not violated.

General oversight and monitoring functions are given to the Access to Information Monitoring Commissioner. Under Article 13, if the individual is not satisfied with the information provided, they can complain to the relevant agency, and if not further satisfied, they may complain to the Access to Information Monitoring Commissioner.

**Law on Mass Media**

Under Article 5 of the Law on Mass Media, which came into force in 2009, every person has the right to seek and obtain “mass media” information, including information from State-run mass media. The government shall provide the information sought by citizens except where the information sought is a military secret and the disclosure of which endangers national security interests.

---

3 Available at http://president.gov.af/sroot_eng.aspx?id=68
The right to privacy is not referred to in the Australian Constitution.

**Privacy Act 1988**

The *Privacy Act 1988 (PA)* is a comprehensive and consolidated privacy law that aims to “promote the protection of the privacy of individuals,” in recognition of the fact that this needs to be “balanced with the interests of entities in carrying out their functions or activities.” Privacy protection is primarily based around the Australian Privacy Principles (APPs) as outlined in Schedule 1 of the PA. The Australian Information Commissioner is the primary privacy authority.

**Scope and application**

Under Section 6, the PA applies to a wide range of organizations and includes both private organizations and government agencies. Under Section 4, the PA expressly applies to the Crown in right of the Commonwealth.

Under Section 6, personal information is broadly defined as including “information or an opinion about an identified individual, or an individual who is reasonably identifiable.” Additional protection is provided to “sensitive information,” which includes an individual’s racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, sexual orientation or practices, criminal record, health information about an individual, genetic information, and biometric information that is to be used for the purpose of automated biometric verification or biometric identification or biometric templates.

**Collection and notification**

Under APP 3.5, an agency must collect personal information only by lawful and fair means. APP 3.6 permits the agency to collect personal information from someone other than the individual if there is consent, if it is required or authorized by a law, or if it is unreasonable or impracticable to do so.

Under APP 3, an agency must not collect personal information unless it is reasonably necessary or directly related to, one of the agency’s functions or activities. For sensitive information, there is an additional requirement for the consent of the individual concerned. However, consent is not required under certain circumstances, including relevantly where:

- the collection is required or authorized by or under an Australian law or court/tribunal order;
- a permitted general situation exists, which relevantly includes, under Section 16A, where the agency has reason to suspect that unlawful activity, or misconduct of a serious nature, relates to the agency’s functions or activities has been, is being or may be engaged in; and the agency reasonably believes that the collection, use or disclosure is necessary in order for the agency to take appropriate action in relation to the matter; or
- the agency is an enforcement body and the collection is reasonably necessary or directly related to one of its enforcement related activities of the agency.


**Privacy and data protection laws** of Bali Process member States
Under APP 5, an agency must take such steps (if any) that is reasonable in the circumstances to notify the individual of certain matters, including:

- the identity of the agency;
- whether the collection is required by law;
- the purpose of the collection;
- the consequences (if any) if the personal information is not collected; and
- any other agency, body or person to whom the agency might usually disclose this type of personal information, including any overseas recipients.

The agency must take these notification steps before, during or as soon as practicable after, the collection of the personal information.

**Use and disclosure**

Under APP 6, information that was collected for a particular primary purpose cannot be used or disclosed for another secondary purpose unless there is consent from an individual or certain circumstances exist. Those exceptional circumstances relevantly include:

- the individual reasonably expects that the information will be used for that secondary purpose, and the secondary purpose is related to the primary purpose;
- the use is required or authorized by an Australian law or court/tribunal order;
- a permitted general situation exists; or
- the agency reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Under APP 6.3, an agency that is not an enforcement body can disclose biometric information to an enforcement body if the disclosure is conducted in accordance with guidelines made by the Australian Information Commissioner.

**Cross-border transfers**

Under APP 8, if an agency makes a cross-border transfer of personal information, the agency must take reasonable steps to ensure that the overseas recipient does not breach the APPs. However, steps do not need to be taken if:

- the agency reasonably believes that the overseas recipient is subject to a law or binding scheme that protects the information in a substantially similar way to the APPs, and that the individual can access and enforce that law or binding scheme;
- the individual consents to the disclosure after being expressly informed of it;
- the disclosure of the information is required or authorized by or under an Australian law or a court/tribunal order;
- a permitted general situation exists; or
- the disclosure of the information is required or authorized by or under an international agreement relating to information sharing to which Australia is a party; or

---

7 See above regarding Section 16A of the PA.
8 Under APP6.5, the agency must make a written note of the use or disclosure under this circumstance.
9 See above regarding Section 16A of the PA.
• the agency reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; and the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Under Section 16C, in certain circumstances, any act done or engaged by the overseas recipient in breach of the APPs is taken to be an act of the originating agency.

Data quality, access and correction

Under APP 10, an agency must take reasonable steps (if any) to ensure that the personal information collected, used and disclosed is accurate, up-to-date, complete and relevant.

Under APP 12, an agency, upon request by an individual, must give access to the personal information held by the agency about the individual. However, the agency can refuse access under the Freedom of Information Act 1982\(^\text{10}\) (FOIA) or other relevant law. Under the FOIA, access and correction procedures for all individuals are established in relation to any personal information about them held by a public sector agency. Relevant exceptions include information:

• relating to personal privacy where disclosure would be contrary to the public interest;
• affecting national security, defence or international relations;
• affecting enforcement of law and protection of public safety;
• containing material obtained in confidence; and
• disclosure of which would be contempt of Parliament or contempt of court.

Under APP 13, if upon a request by an individual to correct their personal information, and an agency is satisfied that information is inaccurate, out of date, incomplete, irrelevant or misleading, the agency must take reasonable steps to correct that personal information. If the agency has disclosed the incorrect information to another APP entity, the individual may request notification to that APP entity of the correction, and the agency must take reasonable steps to do so unless it is impracticable or unlawful to do so.

Retention

Under APP 11, an agency must take reasonable steps to destroy personal information or ensure that it is de-identified if the agency no longer needs the information for the purpose for which it may be used or disclosed, and is not required by an Australian law or court order to retain the information.

Security

Under APP 11, an agency must take reasonable steps to protect personal information from misuse, interference, loss, and unauthorized access, modification or disclosure.

Accountability

Under APP 1, an agency must take such reasonable steps to implement practices, procedures and systems relating to the agency’s functions or activities that will ensure that the agency complies with the APPs and will enable the agency to deal with inquiries or complaints from individuals about the agency’s compliance with the APPs. As part of this, the agency must create an APP privacy policy.

\(^{10}\) Available at http://www.comlaw.gov.au/Details/C2015C00013
Enforcement

Under Part IV of the PA, the AIC’s functions include guidance related functions (publishing guidelines), monitoring related functions, advice related functions, accept complaints from individuals, investigate and assess compliance with the APPs, and determinations enforceable in court.
Bangladesh

The right to privacy is implicitly provided for in the Constitution of the People’s Republic of Bangladesh. Article 43 guarantees the right of the citizen to be “secured in his home against entry, search and seizure” and “to the privacy of his correspondence and other means of communication,” subject to reasonable restrictions imposed by law.

While there is no comprehensive domestic law relating to privacy and data protection, limited protection is provided in right to information legislation.

Right to Information Act 2009

The Right to Information Act 2009 (RTIA) protects information that may offend the privacy of the personal life of an individual from being disclosed. The RTIA applies to information, which is broadly defined, held by “authorities,” which include “any organization/institution constituted in accordance with the Constitution of People’s Republic of Bangladesh,” “any ministry, division or office constituted under the Rules of Business as given in Article 55(6) of the Constitution,” and “any statutory body or institution established by or under any Act.”

Under Article 7, every citizen has a right to information from any authority, subject to a broad number of exceptions. Those exceptions relevantly include any information:

- that may, if disclosed, cause a threat to the security, integrity and sovereignty of Bangladesh;
- relating to any aspect of foreign policy that may affect the existing relationship with any foreign country or international organization or any regional alliance or organization;
- that is secret information received from a foreign government;
- that may, if disclosed, be gainful or damaging to any particular individual or organization;
- that may, if disclosed, obstruct the enforcement of law or incite any offence;
- that may, if disclosed, endanger public security or impede the due judicial process of a pending case;
- that may, if disclosed, offend the privacy of the personal life of an individual;
- given in confidence to any law enforcement agency by a person;
- relating to a pending court matter and which has been expressly forbidden to be published by any court of law or tribunal or the disclosure of which may constitute contempt of court;
- that may, if disclosed, impede the process of investigation;
- that may, if disclosed, affect any investigation process of offence and the arrest and prosecution of offender; or
- that is any secret information of a person which is protected by law.

General oversight and monitoring functions are given to the Information Commission, whose functions include receiving complaints from individuals, conduct investigations, issue directives, procedures and guidelines relating to access to information.

11 Available at http://bdlaws.minlaw.gov.bd/pdf_part.php?id=367
12 Available at www.moi.gov.bd/RTI/RTI_English.pdf
13 Under Article 2(f), information includes any “memo, book, design, map, contract, data, log book, order, notification, document, sample, letter, report, accounts, project proposal, photograph, audio, video, drawing, painting, film, any instrument done through electronic process, machine readable record, and any other documentary material regardless of its physical form or characteristics, and any copy thereof in relation to the constitution, structure and official activities of any authority.”
Bhutan

The right to privacy is implicitly provided for in the Constitution of the Kingdom of Bhutan.\footnote{Available at http://www.bhutanaudit.gov.bt/About%20Us/Mandates/Constitution%20of%20Bhutan%202008.pdf} Article 19 provides that “a person shall not be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence nor to unlawful attacks on the person’s honour and reputation.”

While there is no domestic law relating to privacy and data protection, a Right to Information Bill was passed by the National Assembly in 2014 and is awaiting approval in the National Council.\footnote{The approved Bill is available at http://www.moic.gov.bt/daden/uploads/2014/04/RTI-Bill-Final.pdf}

Brunei Darussalam

The Constitution of Brunei Darussalam focuses on the structure and organization of government, and does not specify individual rights and freedoms, including privacy and privacy related rights.\footnote{Available at www.parliament.am/library/sahmanadrutyunner/bruneydarusalam.pdf}

While there is no comprehensive law relating to privacy and data protection, there are industry specific laws that provide some reference to privacy, such as in banking legislation.\footnote{See commentary at http://www.galexia.com/public/research/assets/unctad_asean_ecommerce_review_2013/unctad_asian_economic_review_2013-BRUNEI.html}

Cambodia

The right to privacy is expressly provided for in the Constitution of the Kingdom of Cambodia.\footnote{Available at http://www.ccc.gov.kh/english/CONSTITUTIONEng.pdf} Article 31 provides for the recognition and respect of “human rights as enshrined in the United Nations Charter, the Universal Declaration of Human Rights and all the treaties and conventions related to human rights, women’s rights and children’s rights.” Article 32 guarantees the “right to life, liberty and security of person.” Article 50 provides that the “protection of the rights to the inviolability of residence and to the confidentiality of correspondences … shall be guaranteed. Search of residences, properties and body search shall be done in accordance with the legal stipulations.”

There is no domestic law relating to privacy and data protection.
China

The right to privacy is implicitly provided for in the People’s Republic of China Constitution and General Principles of the Civil Law. Articles 38 and 40 of the Constitution guarantee privacy related rights such as the right to personal dignity, prohibitions against insult, defamation, false accusation or false information directed against Chinese citizens, inviolability of home, and a right of freedom and secrecy of private correspondence. Article 120 of the General Principles of the Civil Law protects a citizen’s right of personal name, portrait, reputation or honor.

While there is no comprehensive privacy or data protection law applicable to government agencies, privacy and confidentiality are protected in various separate laws and government orders. The 2012 Decision of the Standing Committee of the National People’s Congress on Strengthening Network Information Protection provides arguably the highest level of privacy protection applicable to State bodies. Article 20 of the Decision provides that “State organs and their staff shall protect the secrecy of citizens’ individual electronic information that they learn when carrying out their duties, may not divulge, distort or damage it, and may not sell or illegally provide it to other persons.”

Under the 2011 Provisions on Several Issues regarding Hearing of Administrative Cases Involving Public Government Information issued by the Supreme People’s Court, a citizen can initiate an administrative law action against the government if the citizen considers that publication of information by government infringes upon her or his individual privacy. If the infringement is proven, the disclosure of such information may be declared illegal and remedial measures ordered.

The Regulations on Open Government Information grants citizens the rights of access and correction of personal information. Under Articles 9-12, administrative agencies are required to disclose certain categories of general government information upon their initiative. Under Article 13, citizens may request relevant government information. However, under Article 14, government information relating to national secrets and individual privacy may not be disclosed. Information regarding individual privacy may be disclosed “with the consent of the rightholder or if administrative organs believe that non-disclosure might a major impact on the public interest.”

Under Article 23, if an administrative agency believes that the requested government information involves individual privacy, and disclosing that information might infringe upon the lawful rights and interests of a third party, the agency should seek the third party’s consent. The agency may not disclose the information without consent unless the agency believes that non-disclosure might have a major influence on the public interest. If so, the agency should disclose the information and notify the third party in writing of the content of the disclosed government information and the reasons for disclosure.

Other general protections can be found in the Law of the People’s Republic of China on Resident Identity Cards. Under Article 6, public security organs and police who use citizen’s identity cards must keep the information they obtain from such cards confidential when performing duties or providing services. Under Article 19, administrative sanctions may be given if the police divulge personal information gained through “making, issuing, examining or seizing” an identity card and infringes upon the citizen’s lawful rights and interests.

---

21 An unofficial English translation is available at http://www.law.hku.hk/cprivacy/archives/189
24 Available at http://www.npc.gov.cn/englishnpc/Law/2007-12/05/content_1381969.htm

Privacy and data protection laws of Bali Process member States
Democratic People’s Republic of Korea

The right to privacy is implicitly provided in the Socialist Constitution of the Democratic People’s Republic of Korea. Article 79 guarantees a citizen’s “inviolability of the person and the home, and privacy of correspondence. No citizen can be placed under control or arrest nor can a citizen’s home be searched without a legal warrant.”

There is no domestic law relating to privacy and data protection.

Fiji

The right to privacy is expressly provided for in the Constitution of the Republic of Fiji. Article 24 guarantees the “right to personal privacy, which includes the right to confidentiality of their personal information; confidentiality of their communications; and respect for their private and family life.”

Further, Article 25 guarantees the “right of access to information held by any public office; and information held by another person and required for the exercise or protection of any legal right. Every person has the right to the correction or deletion of false or misleading information that affects that person.” Article 25(3) provides that, to the extent that is necessary, a law may limit, or may authorize the limitation of, these rights and may regulate the procedure under which information held by a public office may be made available.

There is no domestic law relating to privacy and data protection.

---

26 Available at www.pacilti.org/fj/Fiji-Constitution-English-2013.pdf
Hong Kong

The right to privacy is expressly provided for in the Basic Law of the Hong Kong Special Administrative Region. The Basic Law provides for the ongoing application of the ICCPR, which guarantees the individual the right to protection against “unlawful interference with ... privacy, family, home and correspondence.” Furthermore, Article 30 provides:

“The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.”

Additionally, the right to privacy provision of the ICCPR has been incorporated in Bill of Ordinance 1991, which is binding on government authorities.

Personal Data (Privacy) Ordinance 1996

The Personal Data (Privacy) Ordinance 1996 (PDPO) is a comprehensive data regulation that aims to protect individuals’ right to privacy by regulating the handling of personal data in Hong Kong. Privacy protection within the PDPO is primarily founded on six Data Protection Principles (DPP) which are outlined in Schedule 1 of the PDPO. The Privacy Commissioner for Data Protection (PCDP) is the privacy authority.

Scope and application

The PDPO applies to any person or organization, both public and private, that collects, holds, processes or uses personal data. Under Section 3, the PDPO specifically binds the Hong Kong government.

The PDPO defines “personal data” as including any data relating directly or indirectly to a living individual from which it is practicable for the identity of the individual to be directly or indirectly ascertained.

Collection and notification

Under DPP 1, the collection of personal data is limited to collection that is necessary for a lawful purpose directly linked to a function of the data user. The data must also be “adequate but not excessive in relation to that purpose.” Collection must be by lawful means, and “fair in all the circumstances of the case.”

If data is collected from the data subject, the data subject must be given notice of the purpose of collection, consequences of non-provision, and potential recipients of disclosures of the data, access and correction rights and procedures. Notice is not required where personal data is collected from third parties, collected by the way of observing data subject, or provided unsolicited by the data subject. Notification is not required in some exceptional circumstances, including where personal data is held for the purposes of:

- the prevention or detection of crime;
- the apprehension, prosecution or detention of offenders;
- prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons; and
- safeguarding security, defence or international relations in respect of Hong Kong where notification would be likely to prejudice these matters.

**Use and disclosure**

DPP 3 restricts the use, including disclosure, of personal data to purposes for which the data was originally collected, or a directly related purpose, unless the data subject voluntarily gives “prescribed” consent to a new purpose. “Prescribed” consent means the express consent of the person given voluntarily and does not include any consent which has been withdrawn by written notice.

Under Part 8 of the PDPO, broad exceptions to DPP 3 apply, relevantly to use or disclosure of personal data that is:

- required or authorized by any Hong Kong law or court order;
- required in connection with legal proceedings in Hong Kong or exercising or defending legal rights in Hong Kong;
- related to the prevention or detection of crime;
- related to the apprehension, prosecution or detention of offenders;
- related to the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons; and
- held for the purposes of safeguarding security, defence or international relations in respect of Hong Kong where notification would be likely to prejudice these matters.

**Cross-border transfers**

Under Section 33, which is not yet in force, the transfer of personal data from within Hong Kong to a place outside of Hong Kong is prohibited except in certain circumstances. The exceptional circumstances relevantly include where:

- the PCPD has specified the place as having laws in force that is substantially similar to, or serves the same purposes, as the PDPO;
- the data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the PDPO;
- the data subject has consented in writing to the transfer;
- the data user has reasonable grounds for believing that, in all the circumstances of the case:
  - the transfer is for the avoidance or mitigation of adverse action against the data subject;
  - it is not practicable to obtain the written consent of the data subject and
  - if it was practicable to obtain such consent, the data subject would give it;
• the data is exempt from DPP 3 by virtue of an exemption under Part 8 (see above); and
• the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the PDPO.

Matching procedure

Under Section 30, a matching procedure must not be performed unless:

- it is explicitly consented to by the individual;
- it is part of a class of matching procedures that has been approved by the PCPD, and complies with any relevant conditions issued by the PCPD; or
- it is specifically approved by the PCPD.

Under Section 32, when deciding whether to approve a matching procedure, the PCPD must take into account the following prescribed matters:

- whether the carrying out of the matching procedure is in the public interest;
- the kind of personal data used in the matching procedure;
- the likely consequences to a data subject if there is a resulting adverse action;
- the practices and procedures, if any, that will be followed to enable a data subject to make a data correction request;
- the practices and procedures, if any, to ensure the accuracy of any personal data produced or verified by the matching procedure;
- whether any such data subject is to be informed of the procedure before it is first carried out;
- whether there is any practicable alternative to the matching procedure; and
- the benefits to be derived from carrying out the matching procedure.

A data user must not take any adverse action against an individual as a result of a matching procedure unless the data user has notified the individual in writing. The notice must specify the adverse action proposed and the reasons for the action. The individual must be notified that the individual has 7 days after the receipt of the notice to explain why that action should not be taken. However, an exception to this notification requirement arises if notification would prejudice any investigation into the commission of an offence or the possible commission of an offence.

Data quality, access and correction

DPP 2 requires that all practicable steps must be taken to ensure accuracy of personal data, and to erase and not to use inaccurate data. “Inaccurate” data means data that is “inaccurate, misleading, and incomplete or obsolete.” Where inaccurate personal data has been disclosed to a third party, the third party should be informed of that inaccuracy and the means to rectify the data. This requirement to notify third parties only arises where it is practicable to do so.

30 “Matching procedure” means the automated matching of personal data with respect to 10 or more individuals collected for different purposes with the aim of producing or verifying data that may result in the taking of adverse action against the individual concern. Data matching is exclusively performed by the Hong Kong public agencies, particularly in relation to national ID cards.
DPP 6 provides for rights of access to and correction of data. Part 5 of the PDPO provides the procedures for requests for access and correction of personal data. Under Part 8 of the PDPO, relevant exceptions to DPP 6 apply to personal data that is:

- related to the prevention or detection of crime;
- related to the apprehension, prosecution or detention of offenders;
- related to prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons; and
- held for the purposes of safeguarding security, defence or international relations in respect of Hong Kong where notification would be likely to prejudice these matters.31

Retention

DPP 2(2) requires that “personal data shall not be kept longer than it is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are used or are to be used in the future.” Under Section 26(1), a data user must take all practicable steps to erase personal data where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless:

- any such erasure is prohibited under any law; or
- it is in the public interest (including historical interest) for the data not to be erased.

Security

DPP 4 requires that all practicable steps be taken to protect personal data against “unauthorized or accidental access, processing, erasure, loss or use” regarding the kind of data, their physical location, the potential harm from the action listed above, the security measures incorporated, and the measures to ensure the integrity of persons having access to the data.

Accountability

The data user is the person who “controls the collection, holding, processing or use” of personal data and bears responsibility under the PDPO. A party who only processes data as agent of another person is not a data user. This party is a data processor who has a separate obligation to delete personal data once the purpose of processing is complete.

Enforcement

Under Section 5, the PCDP is established as an independent statutory authority. The functions of the PCDP are broadly defined under Section 8 and include supervising compliance with the PDPO, promoting awareness and understanding of the PDPO, examining proposed legislation that might affect individual privacy, and inspecting data systems.

The PCDP may investigate breaches of the PDPO, either upon a complaint or by its own initiation. The PCDP can issue an enforcement notice against the data user and require the data user to take remedial action. Civil or criminal proceedings may be instituted against any data user who fails to comply with an enforcement notice, including financial penalties and imprisonment. The PCDP may also publicly publish the results of any investigation, the name the data user and the details of the breaches.

The right to privacy is implicitly provided for in the Constitution of India. The Supreme Court of India has implied the right to privacy from Article 21, which provides that “no person shall be deprived of his life or personal liberty except according to procedure established by law.”

While there is no consolidated privacy legislation in India, various laws contain provisions that either implicitly or explicitly preserve the right to privacy.

**Information Technology Act 2000**

The most significant and relevant legislation is the Information Technology Act 2000 (ITA), however the privacy protections in the ITA only applies to body corporates and State authorities with powers under the ITA. It does not apply to all government agencies, including law enforcement and immigration agencies.

Section 43A of the ITA provides for protection of sensitive personal data of individuals. A body corporate possessing, dealing with or handling sensitive personal data in a computer resource must implement and maintain reasonable security practices and procedures. If the body corporate is negligent in implementing these security practices and procedures and as a result causes wrongful loss or wrongful gain to any person, it may be required to pay damages to the affected person.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Rules) were established to support Section 43A. The IT Rules established requirements broadly consistent with general privacy principles, including that body corporates establish a publicly available privacy policy, that there be consent in writing, that sensitive personal data is only collected where it is necessary for a lawful purpose, that there be reasonable notification, that information will be used for the purpose for which it was collected, that information be retained only for the lawful purpose, and that individuals can access and correct their personal information.

**Right to Information Act 2005**

The Right to Information Act 2005 (RTIA) provides citizens and legal persons with the right to request information from government bodies. Section 8(1) provides for a wide range of exceptions to this right, including relevantly where information:

- if disclosed would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State, relations with a foreign State or lead to incitement of an offence;
- which has been expressly forbidden to be published by any court of law or tribunal or the disclosure of which may constitute contempt of court;

32 http://india.gov.in/my-government/constitution-india/constitution-india-full-text
33 R. Rajagopal v. State of Tamil Nadu (1994) SCC (6) 632
35 The definition for sensitive personal data was elaborated in Rule 3 of the IT Rules to include “password; financial information such as Bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information.”
37 Available at http://rti.gov.in/rti-act.pdf
• received in confidence from a foreign Government;
• if disclosed would endanger the life or physical safety of any person or identify a confidential source of information given for law enforcement or security purposes;
• if disclosed would impede the investigation, apprehension or prosecution of offenders; or
• which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the relevant authority is satisfied that the larger public interest justifies the disclosure of such information.

However, Section 8(2) provides a further public interest exemption. It states that notwithstanding “anything in the Official Secrets Act, 1923 nor any of the exemptions permissible in accordance with sub-section (1), a public authority may allow access to information, if public interest in disclosure outweighs the harm to the protected interests.”

The Chief Information Commissioner may receive and investigate complaints, conduct inquiries, decide appeals of decisions on requests, and prepare reports on the RTIA.
The right to privacy is implicitly provided for in the Constitution on the Republic of Indonesia.\textsuperscript{38} Chapter 10 provides privacy-related rights relating to the freedom of communication and reception, and the right to possess and retain information under Article 28F. Article 12 of the Act concerning Human Rights (Law 39 of 1999)\textsuperscript{39} also guarantees rights on the freedom of communication and incorporates the international law principles under the UDHR and the ICCPR, including the right to privacy.

While Indonesia does not currently have a comprehensive privacy law, one is currently in development.\textsuperscript{40} Various laws do provide some level of privacy protection, particularly in relation to government agencies.

**Law on Population Administration 2006**

Under Chapter 9 of the Law on Population Administration (Law 23 of 2006),\textsuperscript{41} the legislative basis for the Electronic Identity Card Program, there is a general requirement for personal data held within the national ID card database to be stored, maintained, kept accurate and protected. The Government Regulation implementing the Law on Population Administration (Regulation 37 of 2007)\textsuperscript{42} provides that users of identity card information cannot disclose information publicly without authorization by the relevant Minister.

**Law on Information and Electronic Transactions 2008**

The Law on Information and Electronic Transactions (Law 11 of 2008) (LIET)\textsuperscript{43} provides some privacy protection for electronic information, including those held by public agencies. In particular, Article 26 requires the consent of the individual regarding any use of personal information in any electronic system, unless there is authority from the law. Unauthorized use of electronic information is an offence. The LIET is supported by Government Regulation No. 82 of 2012 regarding Provision of Electronic System and Transaction,\textsuperscript{44} which provides more detail about how Article 26 is implemented. Under Article 15 of this Regulation, an “electronic system operator” (ESO) is required to:

- keep the secrecy, integrity and availability of personal data;
- ensure that the acquisition, use and utilization of personal data is based on approval of the owner of the data, unless otherwise provided by laws and regulations; and
- ensure that the use or disclosure is based on consent and in accordance with purpose notified to the data owner, disclosed to the owner at the time of acquisition.

---

\textsuperscript{38} Available at www.setneg.go.id/images/stories/kepmen/legal_product/uud_1945.pdf

\textsuperscript{39} Unofficial English translation available at http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/65808/105633/F1716745068/IDN65808%20Eng.pdf

\textsuperscript{40} Sinta Dewi, ‘Indonesia’s Plans for Privacy Law’ (2009) 92 Privacy Laws & Business International Newsletter, p17

\textsuperscript{41} Unofficial translation is available at http://www.refworld.org/cgi-bin/textis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=54efefde4

\textsuperscript{42} Original version available at http://www.hukor.depkes.go.id/up_prod_pp/PP%20No.%2037%20Th%202007%20ttg%20Kependudukan.pdf


\textsuperscript{44} Unofficial translation is available at http://rulebook-jica.ekon.go.id/english/4902_PP_82_2012_e.html
An ESO includes a “state agency” that provides, manages, and/or operates an electronic system. Under Article 16 of the Regulation, the ESO for public services is obligated to implement good management and accountability of the electronic system. Under Article 22, the ESO is also responsible to maintain the “confidentiality, integrity, authenticity, accessibility, availability and traceability” of the electronic information.

**Public Information Disclosure Act 2008**

The Public Information Disclosure Act 2008\(^45\) (PIDA) provides for the right access to information held by public agencies, and requires public agencies to proactively publish information as well as to release information upon request. This right only applies to Indonesia citizens or entities.

Under Article 1.3, a public agency includes “executive, legislative, judicative and other agencies whose function and main duties are related to the organizing of the state, where part or all of its funds originate from the state budget and/or the regional budget, or a non-governmental organizations that part or all of its fund originate from the state budget and/or the regional budget, the contribution from the people and/or from overseas sources.”

Under Article 6, public agencies may refuse to provide:

- classified information pursuant to the provisions and regulations of the laws; and
- public information if it is not in accordance with laws and regulations, namely public information that may jeopardize the state, information relating to personal rights or office secrets, and public information not within the public agency’s authority or has not yet been documented.

Further exceptions arise under Article 17 in relation to public information, including relevantly, information that may:

- obstruct the process of law enforcement;
- be hazardous to the defense and security of the state;
- be harmful to diplomatic relations;
- reveal a personal secret;\(^46\) or
- not be disclosed under the law.


\(^46\) Personal secrets can include the history and condition of a member of the family; the history, condition and care, physical medical treatment, and physic of an individual; the memorandum or letters between the public agencies or among the public agencies that, based on their nature are confidential.
Iran

The right to privacy is implicitly provided for in the *Islamic Republic of Iran Constitution.* Article 22 guarantees that the “dignity, life, property, rights, residence, and occupation of the individual are inviolate, except in cases sanctioned by law.” Article 25 provides for the protection of correspondence and communications from inspection by the state, except as provided by law.

There is no domestic law relating to privacy and data protection.

Iraq

The right to privacy is expressly provided for in the *Irani Constitution.* Article 17 guarantees the “right to personal privacy so long as it does not contradict the rights of others and public morals.” Article 17 also ensures that “the sanctity of the homes shall be protected. Homes may not be entered, searched, or violated, except by a judicial decision in accordance with the law.”

There is no domestic law relating to privacy and data protection.
Japan

The right to privacy is implicitly provided for in the Constitution of Japan. Article 13 guarantees that “all of the people shall be respected as individuals. The right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation in other governmental affairs.”


The Act on the Protection of Personal Information 2003 (APPI) and the Act on the Protection of Personal Information Held by Administrative Organs 2003 (APPIHAO) are complementary and comprehensive laws that aims to “protect the rights and interests of individuals while taking consideration of the usefulness of personal information.” No independent privacy authority is established under the APPI or the APPIHAO. Enforcement responsibility under the APPI is generally given to a “competent minister,” being the minister with jurisdiction over the business of the business operator.

Scope and application

The APPI protects “personal information,” which is broadly defined, held by “business operators,” which relevantly includes State organs and local governments. Under Article 4, the State has broad responsibility for “comprehensively formulating and implementing measures necessary for ensuring the proper handling of personal information in conformity with the purpose of this Act.”

The APPIHAO also protects personal information but applies more specifically to “administrative organs,” which includes organs within the cabinet or under the jurisdiction of the Cabinet and organs under the National Government Organization Act. This report will focus on the APPIHAO given its specific applicability to administrative organs. Under the APPIHAO, the head of the administrative organ (Head) is generally responsible for the obligations of administrative organs.

Collection and notification

Under Article 3 of the APPIHAO, an administrative organ shall specify the purpose of use of personal information as much as possible. The administrative organ “shall not change the Purpose of Use beyond the scope which is reasonable to find that the changed Purpose of Use is appropriately relevant to the original Purpose of Use.”

---

49 http://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html
50 Available at http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf
51 Available at http://www.cas.go.jp/jp/seisaku/hourei/data/APPIHAO.pdf
52 Personal information means “information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information including such (information as will allow easy reference to other information and will thereby enable the identification of the specific individual).”
Under Article 4 of the APPIHAO, an administrative organ shall clearly indicate the Purpose of Use to the person. Relevant exceptions exist where:

- collection is urgently required for the protection of the life, body property of an individual;
- notification of the Purpose of Use is likely to cause harm to the life, body, property, or other rights or interests of the individual or a third party;
- notification is likely to cause impediments to the proper execution of the affairs or business of state organs; and
- the Purpose of Use is found to be clear in light of the circumstances of the collection.

Article 18 of the APPI is substantially similar to Article 4 of the APPIHAO, with the additional exception of cases where the handling of personal information by a business operator is necessary for cooperating with a state organ in executing the state organ’s affairs as prescribed by laws and regulations, and the obtaining of consent is likely to impede the execution of such affairs.

Under Article 10 of the APPIHAO, the Head must notify the Minister of Internal Affairs and Communications when it intends to retain computerized information systems (known as a Personal Information File under the APPIHAO). The Head must provide notification of the name of the Personal Information File, the purpose of the use, method of collection, whether the information will be routinely provided to a third party, and procedures to meet requests for access and correction. However, notification under Article 10 is not required in certain circumstances, including where the personal information file is prepared or obtained for criminal investigations, or it contains matters concerning security, diplomatic secrets and other important interests of the State.

Under Article 11, the Head must then prepare and public a register of the Personal Information File with certain particulars, except for Personal Information Files that:

- fall within those exceptional circumstances under Article 10; or
- the publication of the registry entry is likely to cause considerable impediments to the proper execution of the affairs pertaining to the Purpose of Use due to the nature of the said affairs.

**Use and disclosure**

Under Article 8 of the APPIHAO, the Head shall not use or disclose retained personal information for purposes other than the Purpose of Use, unless otherwise provided by laws and regulations. Further exceptions exist, however those exceptions do not apply where the use for another purpose is likely to cause unjust harm to the rights or interests of the individual concerned or a third party. Otherwise, the relevant exceptions include where:

- there is consent of the individual;
- the retained personal information is provided to the individual;
- the retained personal information is used within the administrator organ only to the extent necessary for executing the affairs under its jurisdiction provided by laws and regulations, and there is a reasonable ground for such use of the information; and
- the retained personal information is provided to another administrative organ in which the person who receives the information uses it only to the extent necessary for executing the affairs or business under its jurisdiction, and there is a reasonable ground for such use of the information.
Additionally, under Article 23 of the APPI, another exceptional circumstance is where the handling of personal information is necessary for cooperating with a state organ in executing the state organ’s affairs as prescribed by laws and regulations, and the obtaining of consent is likely to impede the execution of such affairs.

Under Article 9 of the APPIHAO, the Head may impose restrictions or request necessary measures when disclosing to a third party for the proper management of the information.

**Cross border transfers**

There is no specific provision for cross-border transfers of personal information and it appears that any cross-border transfers would generally be provided under the general disclosure provisions above.

**Data quality, access and correction**

Under Article 5 of the APPIHAO, the Head shall endeavor to maintain the retained personal information “consistent with the past or the present facts within the scope necessary for the achievement of the purpose of use.” Substantially similar requirements on the Head are provided under Article 5 of the APPI.

Under Article 14 of the APPIHAO, when a Head is requested by a person to disclose such retained personal information, the Head shall disclose the retained personal data except in relation to non-disclosure information. Non-disclosure information includes information that:

- is likely to harm the life, body, property, or other rights or interests of the person or third party;
- might identify another individual (subject to some further requirements);
- as reasonably considered by the Head, if disclosed is likely to cause harm to national security, cause damage to the relationship of mutual trust with another country or an international organization, or cause a disadvantage in negotiations with another country or an international organization;
- as reasonably considered by the Head, if disclosed is likely to cause impediments to prevention, suppression or investigation of crimes, the maintenance of prosecutions, the execution of punishment, and other matters concerning maintenance of public safety and public order.

Under Article 15, where it is possible to easily “divide and exclude” non-disclosable information for other retained personal information, the Head must provide partial disclosure of the remaining retained personal information.

Under Article 29 of the APPIHAO, a Head must correct retained personal information upon a request by a person to correct, add, or delete such retained personal information and upon finding that there are grounds for the request. Under Article 30 of the APPIHAO, the Head must notify the individual of the outcome of the request.
Under Article 36 of the APPIHAO, a person can request the suspension of use, deletion, or suspension of provision of retained personal information for several reasons, including violations of Article 3 (retention beyond scope) and Article 8 (use and disclosure without consent). Under Article 38, if the Head considers that there are grounds to the request, suspension will be implemented to ensure the proper handling of the retained personal information. However, this will not apply where suspension is “is likely to hinder the proper execution of the affairs pertaining to the Purpose of Use of the Retained Personal Information due to the nature of the said affairs.”

The Law Concerning Access to Information Held by Administrative Organs 1996\(^{54}\) provides substantially similar rights to access and correction, and exceptions to those rights.

**Retention**

Article 3 of the APPIHAO provides that personal information will only be retained when it is necessary for performing the affairs under the administrative organ’s jurisdiction provided by laws and regulations. Personal information will not be retained beyond the scope necessary to achieve the purpose of use.

**Security**

Under Article 6 of the APPIHAO, a Head shall take necessary and proper measures for the prevention of leakage, loss, or damage and for the proper management of the retained personal information. This requirement applies to individuals or business operators entrusted by an administrative organ with the handling of personal information.

**Accountability**

Heads bear the majority of the responsibility under the APPIHAO.

**Enforcement**

Under Article 48, the Head shall endeavor to properly and expeditiously process complaints about the handling of personal information.

Under Article 49, the Minister of Internal Affairs and Communications may collect reports on the status of enforcement of the APPIHAO from the heads of administrative organs. The Minister of Internal Affairs and Communications shall then annually compile the reports and make public a summary of them.

Under Chapter 6 of the APPIHAO, certain penal provisions exist for employees who unlawfully disclose personal information without justifiable grounds, persons who disclose or appropriates retained personal information for illicit gain, and persons who received retained personal information by deception or other wrongful means.

Under Article 34 of the APPI, when a business operator handling personal information has violated certain provisions relating to the protections described above, the competent Minister may recommend that the business operator handling personal information cease the violation and take other necessary measures to correct the violation when a competent Minister finds it necessary for protecting the rights and interests of individuals.

\(^{54}\) Available at http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/translation4.htm

Privacy and data protection laws of Bali Process member States
If a business operator has received a recommendation and does not take the recommended measures without justifiable ground, and if the competent minister finds that the serious infringement on the rights and interests of individuals is imminent, the competent minister may order the business operator handling personal information to take the recommended measures.

If the competent minister finds it necessary to take measures urgently where there is a serious infringement of the rights and interests of individuals, the competent minister may proceed to issue an order, without a prior recommendation, to the business operator handling personal information to cease the violation and take other necessary measures to rectify the violation.
The right to privacy is implicitly provided for in privacy-related provisions of the Constitution of The Hashemite Kingdom of Jordan. Article 10 provides that “dwelling houses shall be inviolable and shall not be entered except in the circumstances and in the manner prescribed by law.” Article 18 provides that “all postal, telegraphic and telephonic communications shall be treated as secret and as such shall not be subject to censorship or suspension except in circumstances prescribed by law.”

While there are no comprehensive domestic laws relating to privacy and data protection, there are some access and correction rights provided under right to information legislation. Additionally, there are some confidentiality obligations in relation to electronic transactions, banking, employment and some professional associations.

**Law on Securing the Right to Information Access 2007**

The Law on Securing the Right to Information Access 2007 (LSRTIA) provides for citizens with “lawful interest or justification” to request access to information from public authorities. A public authority includes “the ministry, department, authority, entity or any public institution, public official institution or company that is in charge of the management of a public facility.” Exceptions to the right to access include information relating to:

- the nature of religious, racial, ethnic, sexual or color discrimination;
- the secrets and documents protected under another legislation;
- the documents classified as confidential and protected and to be granted by an agreement with another country;
- the secrets related to national defense, state security or foreign policy;
- the personal information and files related to educational or medical persons, professional records, bank accounts and transfers and professional confidentiality;
- the correspondences with personal or confidential nature with governmental departments and the replies thereto;
- the information whose disclosure will affect negotiations between the Kingdom and any other state or authority; and
- the investigations made by the prosecution, judicial system or security authorities concerning any crime or lawsuit within their scope of power.

Under Article 6, an Information Commissioner may receive complaints from individuals requesting information, and may present the complaint to an Information Board for resolution. Both the Information Commissioner and the Information Board have various other management and reporting functions under the LSRTIA.

---

55 Available at http://www.kinghussein.gov.jo/constitution_jo.html
57 See commentary at http://www.worldlaw.org/int/journals/EPICPrivHR/2006/PHR2006-The-4.html
58 Available at http://www3.telus.net/index100/jordanfoi
Kiribati

The right to privacy is implicitly provided for in the Constitution of Kiribati. Article 9 protects the privacy of home and other property. It provides that “except with his own consent, no person shall be subjected to the search of his person or his property or the entry by other others on his premises.” Article 9 also provides that any act contained in or done under the authority of certain laws is deemed to be not inconsistent with this provision. Those laws must make provision in relation to various purposes, for example, the interests of “defence, public safety, public morality, public health,” “protecting the rights or freedoms of other persons,” and “entry upon any premises for the purpose of preventing or detecting criminal offences.”

There is no domestic law relating to privacy and data protection.

Lao People’s Democratic Republic

The right to privacy is implicitly provided for in the Constitution of Lao People’s Democratic Republic. Article 42 provides that “the right of Lao citizens in their bodies, honour and houses are inviolable.”

There is no domestic law relating to privacy and data protection.

59 Available at http://www.parliament.gov.ki/content/constitution-kiribati
Macao

The right to privacy is expressly provided for in the Basic Law of the Macao Special Administrative Region. Article 30 provides that the “human dignity of Macao residents shall be inviolable” and that “Macao residents shall enjoy the right to personal reputation and the privacy of their private and family life.” Article 31 provides that “the homes and other premises of Macao residents shall be inviolable Arbitrary or unlawful search of, or intrusion into, a resident’s home or other premises shall be prohibited.”

Article 32 provides that “the freedom and privacy of communication of Macao residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with the provisions of the law to meet the needs of public security or of investigation into criminal offences.”

Personal Data Protection Act 2005

The Personal Data Protection Act 2005 (PDPA) “establishes the legal system on the processing and protection of personal data,” and is guided by the general principle under Article 2 that “the processing of personal data shall be carried out transparently and in strict respect for privacy and for other fundamental rights, freedoms and guarantees enacted in the Basic Law of the Macao Special Administrative Region, the instruments of international law and the legislation in force.” The PDPA is administered by the Office of Personal Data Protection (OPDP).

Scope and application

The PDPA protects “personal data,” being information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person (the “data subject”). Protections additionally apply to sensitive data, which is characterized as “data revealing philosophical or political beliefs, political society or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data.”

The PDPA applies all data controllers, including those within government agencies. A data controller means the natural or legal person, public entity, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. A data “processor” shall mean a natural or legal person, public entity, agency or any other body which processes personal data on behalf of the controller. Under Article 17, any processor must not process data except on the basis of instruction from the controller unless required to do so by law.

Collection and notification

Under Article 5, data must be collected for specified, explicit and legitimate purposes that are directly related to the activity of the controller.
Under Article 11, the controller must inform the data subject at the time of collection or at least before it is disclosed to a third party various matters, including the identity of the controller, the purpose of the processor, the recipients or categories of recipients of the information, whether the collection is obligatory or voluntary, the possible consequences if data is not collected, and the existence and conditions of the right of access and rectification. This obligation to inform may be relevantly waived where there is a “legal provision” or “on the grounds of security and criminal prevention or investigation.”

Under Article 21, notification must be made to the OPDP of automated processing of data or processing of sensitive data, unless exemption from notification is obtained from the OPDP.

Use and disclosure

Under Article 5, personal data must be processed lawfully and in good faith, and must not be processed in a way that is “incompatible” with the original purpose of collection. Further, under Article 6, personal data may be processed only if the data subject has unambiguously given consent unless it is necessary in the following relevant circumstances for:

- compliance with a legal obligation to which the controller is subject;
- performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; and
- pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

Under Article 7, the processing of sensitive personal data is prohibited except where, relevantly:

- the data subject has given explicit consent for such processing;
- there is explicit authorization by a legal provision or regulation;
- on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller, and is authorized by the OPDP;
- sensitive personal data was made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations; and
- processing is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose.

Further provisions relating to processing of data in relation to enforcement activities are found in Article 8. Registers of personal data relating to “illegal activities, criminal and administrative offences, and decisions applying penalties, security measures, fines and additional penalties” may only be established by public services where there is specific legal provision or statutory regulation. The register must also be subject to procedural and data protection rules in force.

Processing of data within these registers is permitted when it is necessary for pursuing the legitimate purposes of the controller, provided the fundamental rights and freedoms of the data subject are not overriding. Processing for police investigations is restricted to where it is necessary to prevent a specific danger, to prosecute a particular offence, and to exercise responsibilities arising from a legal provision, statutory regulation, or an international law or inter-regional agreement.

Under Article 17, any processor must not process personal data except on the basis of instructions from the controller, unless required to do so by law.
Cross-border transfers

Under Article 19, the transfer of personal data to an outside destination must comply with the PDPA and only where the destination has a legal system that ensures an adequate level of protection, as determined by the OPDP. An adequate level of protection is not required where, relevantly:

- there is unambiguous consent from the data subject and the OPDP is notified;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment or defence of legal claims; or
- the public authority authorizes a transfers of personal data to the destination, provided the data controller adduces adequate safeguards to protect privacy and fundamental rights and freedoms of individuals, particularly through appropriate contractual clauses.

Under Article 20(3), where the transfer of personal data is necessary for the protection of defence, public security and public health, and for the prevention, investigation and prosecution of criminal offences, the transfer shall be governed by “special legal provisions” (which appears to refer to any specific legal provisions within other legislation that authorize transfers) or by the international conventions and regional agreements to which Macao is party.

Automatic processing

Under Article 9, automatic processing, or the “combination of personal data,” shall by subject to the authorization of the OPDP, unless it is provided for in a legal provision or a statutory regulation. In order for the “combination of personal data” to be authorized, it must:

- be necessary for pursuing the legal or statutory purposes and legitimate interests of the controller;
- not involve discrimination or a reduction in the fundamental rights and freedoms of the data subjects;
- be covered by adequate security measures; and
- take account of the type of data subject to combination.

Under Article 13, individuals have the right to be not subject to decisions with legal effect that is based solely on automated processing of data intended to evaluate personal aspects relating to the individual. However, an individual may be subject to an automated decision if the decision is:

- made during the performance of a contract, provided that performance of the contract has been satisfied, or that there are suitable measures to safeguard the individual’s legitimate interests, including arrangements allowing the individual to “put his point of view”; or
- authorized by a legal provision which shall lay down measures to safeguard the data subject’s legitimate interests.

Data quality, access and correction

Under Articles 10 and 11, there is a right to access and an obligation to provide information. This right may be waived where there is a legal provision otherwise or there are grounds of security and criminal prevention or investigation. For cases of data processing relating to security and criminal prevention or investigation, the right of access is exercised by a “competent authority,”63 and not the individual.

---

63 The PDPA does not define or outline what is a competent authority.
Under Article 12, the data subject has the right to object at any time on compelling legitimate
grounds to the processing of data relating to him, and where there is a justified objection the
processing instigated by the controller may no longer involve those data. An exception exists if the
processing is otherwise provided by law.

Retention

Under Article 5, personal data must be kept in an identifiable form for no longer than is
necessary for the purposes for which the data was collected or further processed. The storing of
data for historical, statistical or scientific purposes for longer periods may be authorized by the
ODPD at the request of the controller in the case of a legitimate interest.

Security

Under Article 15, the controller must provide appropriate measures to protect personal data from
accidental or unlawful destruction, alteration, loss, and unauthorized access and disclosure. Such
measures must ensure a level of security appropriate to the risks represented by the processing and
nature of the protected data.

Enforcement

The OPDP is the privacy authority operating as a supervising authority under Macao’s chief
executive. It can exercise all power attributed to the “public authority” under the PDPA. The ODPD
does not currently have any separate legislation to establish it as an independent authority, or
regulations on how it will exercise its powers.

Under the Chapter VIII of the PDPA, administrative and criminal fines and sanctions apply to
breaches of the PDPA. Under Article 14, individuals also have a general right to indemnification
if they have suffered damage as a result of an unlawful processing operation or of any other act
incompatible with the PDPA.
Malaysia

The right to privacy is implicitly provided for in the Federal Constitution of Malaysia through Article 5(1) which states that “no person shall be deprived of his life or personal liberty, save in accordance with law.”

**Personal Data Protection Act 2010**

The Personal Data Protection Act 2010 (PDPA) is a consolidated privacy law that applies only to the private sector in relation to commercial transactions. Under Section 3(1), the PDPA explicitly does not apply to government agencies. Under Section 45(2)(e), there is further broad exemption from the PDPA of any data processing by commercial organizations for the purpose of discharging regulatory functions or obligations. Taken together, this means that no law enforcement or immigration related activities, including those contracted out to third parties, would fall within the scope of the PDPA.

Maldives

The right to privacy is expressly provided for generally in the Constitution of the Republic of Maldives 2008. Article 24 guarantees the right of respect for a “person’s private and family life, home and privacy communications.”

While there is no comprehensive domestic law relating to privacy and data protection in the Maldives, limited protection is provided in the Right to Information Act 2014 (RITA).

**Right to Information Act 2014**

The RTIA provides for a general right to access and correct personal information held by a “state office,” subject to certain exemptions. The relevant exceptions against disclosure upon a request include:

- under Article 22, disclosures of information which is an offence under any law of the Maldives, could cause action for breach of confidence to be filed against the government or could prevent future communication of such information to the government;
- under Article 23, personal information without the consent of the individual concerned; and
- under Article 27, records relating to enforcement activities, including information containing details that could prejudice an ongoing investigation of an alleged breach of law, confidential information for the enforcement or administration of legislation, information that could prejudice the effectiveness of a lawful method or procedure for preventing, detecting, investigating or dealing with acts constituting a breach of law.

---

64 Available at http://www.agc.gov.my/images/Personalisation/Buss/pdf/Federal%20Consti%20(B1%20text).pdf; The right to privacy was accepted as part of the right to personal liberty in the Federal court case Sivarasa Rasiah v. Badan Peguam Malaysia & Anor [2010] 3 CLJ 507 at 519.
65 Available at http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf
The Information Commissioner may publish guidelines for the RTIA, receive complaints and determine appeals from decisions on accessing and correcting personal information, and produce annual reports on the implementation of the RTIA.

Mongolia

The right to privacy is implicitly provided for in the Constitution of Mongolia. Article 13 guarantees “the right to personal liberty and safety.” Article 13 also provides that “no one may be searched, arrested, detained, persecuted, or restricted of liberty save in accordance with procedures and on grounds determined by law” and “privacy of citizens, their families, correspondence, and homes are protected by law.”

Law on the Information Transparency and Right to Information 2011

While there is no comprehensive law relating to privacy and data protection, individuals have the right to access information under the Law on the Information Transparency and Right to Information 2011 (LITRI). Under Article 3.2, the LITRI specifically does not apply to “armed forces, border protection and internal troops, and intelligence organizations.”

Under Article 11 of the LITRI, citizens and legal entities shall be entitled to receive information about the activities of a public organization unless exceptional circumstances arise. Those exceptional circumstances include where:

- disclosure is prohibited by law to ensure human rights, freedom, national security, and organization's lawful interest from the organization;
- disclosure might be detrimental to the national security and public interest of Mongolia;
- it is necessary to protect the secrets of state, organization and individual during the process of inquiry, investigation and prosecution;
- the information is related to the process of concluding international treaty or agreement;
- disclosure is not required under laws and legislations; and
- unless otherwise provided by law, an individual has not agreed in written, (except for information of his/her parents’ name, first name, age, gender, profession, education, official position, work address and telephone number).

Under Article 17, complaints regarding violations of the rights of citizens and legal entities may be made to a “higher level organization or official, the National Commission for Human rights, or a court.”

---

Myanmar

The right to privacy is expressly provided for generally in the Constitution of the Republic of the Union of Myanmar. Article 357 protects “the privacy and security of home, property, correspondence and other communications of citizens under the law,” subject to the provisions of the Constitution.

There is no domestic law relating to privacy and data protection.

Nauru

The right to privacy is expressly provided for in the Constitution of Nauru. Section 3 guarantees the rights to “life, liberty, security of the person” and “respect for his private and family life.”

There is no domestic law relating to privacy and data protection.
Nepal

The right to privacy is expressly provided for in the *Interim Constitution of Nepal*. Article 28 provides that “except in circumstances as provided by law, the privacy of the person, residence, property, document, statistics, correspondence, and character of anyone is inviolable.”

**Right to Information Act 2007**

The *Right to Information Act 2007* (RTIA), in addition to providing the right to access individual information held by “public bodies,” also provides a strong level of privacy protection in relation to information held by public bodies.

Under Section 3, Nepalese citizens have the right to access information held by public bodies, subject to some exemptions. The relevant exemptions relate to information that:

- seriously jeopardizes the sovereignty, integrity, national security, public peace, stability and international relations of Nepal;
- directly affects the investigation, inquiry and prosecution of crimes;
- jeopardizes the harmonious relationship subsisted among various cast or communities; and
- interferes with individual privacy and security of body, life, property or health of a person.

Under Section 27, a committee is established to ensure the protection of these types of exempt information. The committee is to inform the National Information Commission of the period that the information should be kept confidential (with a maximum of 30 years), and the method for the protection of the information.

Under Section 35, individuals may seek correction of any information that is incorrect.

Under Section 28, a public body shall protect the information of a personal nature from unauthorized publication and broadcasting. Further, personal information shall not be used without written consent of the person concerned except in the following circumstances:

- preventing of a serious threat to life and body of a person or public health or security;
- necessary to be disclosed in accordance with prevailing laws; and
- necessary to control the offence of corruption.

Under Section 31, a person who obtains information from a public body shall not misuse the information by not using it for the same purpose that was considered. The concerned public body may complain to the National Information Commission against a person who misuses the information. The National Information Commission may also hear appeals, fine officers of a public body, and order compensation.

---


New Caledonia

New Caledonia is an overseas territory of France. While not all laws of France automatically apply to New Caledonia, the French Data Protection Act 1978 (DPA)\(^4\) expressly applies to New Caledonia.

**Data Protection Act 1978**

The DPA is a comprehensive and consolidated privacy law that was amended in 2004 to comply with the EU Directive. The DPA is guided by the overall principle under Article 1, which states that:

> “Information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties.”

The DPA provides for procedures ensuring the confidentiality of personal information held by government agencies and private entities. It also established an independent data protection authority, the Commission Nationale de l’Informatique et des Libertés (CNIL).

**Scope and application**

Under Article 2, personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to them. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

Under Article 3, a data controller means “a person, public authority, department or any other organisation who determines the purposes and means of the data processing.”

**Collection and notification**

Under Article 6, data controllers must ensure that all personal data collected is processed fairly and lawfully and collected for specified, explicit and legitimate purposes.

Under Article 23, data controllers must provide notification to the NCIL about any data processing regarding compliance with the requirements of the law. Article 24 provides for “simplified notification” to the NCIL of “most common categories of processing of personal data, which is not likely to be a violation of privacy or liberties.” The NCIL may determine categories of processing that are exempt from the notification obligation by taking account of their purposes, recipients or categories of recipients, the personal data processed, the retention period of the data and the categories of the data subjects.

\(^4\) Available at http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf
Under Article 25, a data controller must notify the CNIL if it intends to process data for the following relevant purposes:

- automatic processing of genetic data;
- processing of data relating to offences, convictions or security measures, except for those carried out legal representatives when defending data subjects;
- automatic processing which may exclude persons from the benefit of a right, a service or a contract in the absence of any legislative or regulatory provision;
- automatic processing to combine files of one or several legal entities who manage a public service and whose purposes relate to different public interests;
- automatic processing for assessments of the social difficulties of natural persons; and
- automatic processing of biometric data necessary for the verification of an individual’s identity.

Under Article 26, exceptions to this requirement arise where processing:

- involves State security, defence or public safety; or
- is for the purpose of prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of criminal sentences or security measures.

Furthermore, Article 27 permits the Conseil d’Etat (Council of State) to authorize the processing of personal data carried out on behalf of the State, upon a reasoned and published opinion of the CNIL, relating to:

- data containing the registration number of individuals in the national register for the identification of individuals; and
- biometric data necessary for the identification or verification of the identity of individuals.

**Use and disclosure**

Under Article 7, processing of personal data must have received the consent of the data subject or must meet one of the following conditions:

- compliance with any legal obligation to which the data controller is subject;
- the protection of the data subject’s life;
- the performance of a public service mission entrusted to the data controller or recipient;
- the pursuit of the data controller’s or the data recipient’s legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject.

Under Article 8, the processing of sensitive personal data is prohibited unless, relevantly:

- the data subject has given consent;
- processing is necessary to protect human life and the data subject is unable to give consent due to legal incapacity or physical impossibility;
- personal data has been made public by the data subject; or
- processing is necessary for the establishment, exercise or defence of a legal claim.

---

75 Under Article 8, sensitive personal data means the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or which concern their health or sexual life.
Under Article 9, the processing of personal data relating to offences, convictions and security measures may be put in place only by:

- the courts, public authorities and legal entities that manage public services, within the framework of their legal jurisdiction; and
- the representatives of the law for the strict needs of the exercise of the functions granted to them by the law.

### Cross-border transfers

Under Article 68, transfer to a country outside the European Union is only permitted if the country guarantees individuals a sufficient level of protection of individuals’ privacy, liberties and fundamental rights with regard to the actual or possible processing of their personal data.

Article 69 provides that data can be transferred to a country without an adequate level of protection in certain exceptional circumstances, including where:

- the data subject has provided consent to their data being transferred; or
- the transfer is necessary:
  - for the protection of the individual’s life;
  - for the protection of the public interest;
  - to comply with obligations relating to acknowledgement, exercise or defence of a legal right;
  - for consultation of a public register intended for the public’s information; or
- subject to the CNIL authorizing the transfer, there is a guarantee of a sufficient level of protection of individuals’ privacy as well as their liberties and fundamental rights, particularly on account of contractual clauses or internal rules relating to the processing.

### Automatic processing

Under Article 22, automatic processing of personal data must be notified to the CNIL except when:

- notification is not required under Articles 25, 26 and 27 as described above;
- the sole purpose of the processing is the keeping of a public information register according to laws or regulations and is open for public consultation or by any person demonstrating a legitimate interest; or
- the data controller has appointed a personal data protection officer charged with ensuring, in an independent manner, compliance with the obligations relating to notification to the NCIL under Articles 23 and 24, except where a transfer of personal data to a non EU member State.

### Data quality, access and correction

Under Article 6, controllers must ensure that personal data is adequate, relevant, and non-excessive in view of the purposes for which it is collected, and accurate, comprehensive and kept up-to-date.

Under Article 39, a data subject may request personal data held by the data controller, and request to be informed of:

- whether the personal data relating to him are part of the processing;
- the purposes of the processing, the categories of processed personal data, and the recipients or categories of recipients to whom the data are disclosed;
• the intended transfer of personal data to a State that is not a Member State of the European Union, if applicable;
• the personal data relating to him and any available information on the origin of the data; and
• information allowing him to learn of and object to the reason for automatic processing, in the case of a decision taken based on automatic processing and producing legal effects in relation to the individual.

Under Article 40, the data subject may also request the data controller to correct, complete, update, block, or delete personal data that is inaccurate, incomplete, equivocal, or obsolete, or whose collection, use, disclosure, or storage is prohibited.

Under Article 41, where the data processing is related to the security of the state, defense, or public security, the data subject has a right of indirect access through the CNIL. The CNIL checks and verifies the relevance and accuracy of the data, and may demand correction or deletion. If the data controller agrees, the data may also be disclosed to the data subject by the CNIL.

Retention

Under Article 6, personal data may not be stored beyond the period necessary for the purposes for which they are obtained and processed.

Security

Under Article 34, the data controller must take all useful precautions with respect to the nature of the data and the risk presented by the processing to preserve the security of the data and, among other things, prevent the alteration, corruption or access by unauthorized third parties.

Accountability

Under Article 35, a data processor may only process personal data on behalf of, and on instruction by, the data controller. The data processor must provide sufficient guarantees in terms of security and confidentiality but, ultimately, the data controller is liable for compliance and accountable for any breaches.

Enforcement

Under Article 11, the CNIL’s primary purpose is to inform all data subjects and data controllers of their rights and duties; and ensure that the processing of personal data is carried out in conformity with the provisions of the DPA. If there is any non-compliance with the DPA, the CNIL may issue warnings, or order financial sanctions, injunctions or imprisonment.
New Zealand

New Zealand does not have a written constitution.

Privacy Act 1993

The Privacy Act 1993 (PA)\(^\text{76}\) is a comprehensive and consolidated privacy law that aims to “promote and protect individual privacy” by creating a legal framework to regulate handling of personal information. This legal framework is based around compliance with 12 Privacy Principles (PP) as set out in Part 2 of the PA. The Privacy Commissioner is the primary privacy authority.

Scope and application

The PA applies to “individuals,” which is broadly defined to mean natural living persons, and to “personal information,” which is broadly defined to be any information about an identifiable individual. The PA applies to both public and private sectors, and binds the Crown.

Collection and notification

Under PP 1, personal information shall not be collected by any agency unless:

- the information is collected for a lawful purpose connected with a function or activity of the agency; and
- the collection of the information is necessary for that purpose.

Under PP 2, personal information shall be collected directly from the individual concerned.

Under PP 3, an agency must ensure that the individual concerned is aware of certain matters, including that information is being collected, the purpose of the collection, the intended recipients of the information, whether collection is mandated or authorized by law, the contact details of the collecting agency, the consequences of not providing the information, and the access and correction rights available to the individual. This information is to be notified to the individual before or as soon as practicable after the collection of information.

An agency does not have to comply with PP 2 or PP 3 in certain circumstances. These exceptional circumstances relevantly include, where the agency believes, on reasonable grounds, that:

- the information is publicly available information;
- the individual concerned authorizes collection of the information from someone else;
- non-compliance is necessary to avoid prejudice to:
  - the maintenance of the law by any public sector agency (including the prevention, detection, investigation, prosecution, and punishment of offences);
  - the enforcement of a law imposing a pecuniary penalty;
  - the protection of the public revenue;
  - the conduct of proceedings before any court or tribunal;
- compliance would prejudice the purposes of the collection; or
- compliance is not reasonably practicable in the circumstances of the particular case.


Privacy and data protection laws of Bali Process member States
Under Section 54, the Privacy Commissioner may also authorize collection that would otherwise be inconsistent with PP 2 in circumstances where it is in the public interest or beneficial to the individual, unless the individual has expressly refused to authorize the collection for that purpose.

Under PP 4, personal information shall not be collected by an agency by unlawful means, or by means that are unfair, or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Use and disclosure

Under PP 10, personal information that has been collected for one purpose can only be used for another purpose in certain circumstances. Under PP 11, an agency can only disclose personal information to another person in certain circumstances. The exceptional circumstances for both PP 10 and PP 11 are substantially the same and relevantly include where:

- the information is publicly available information;
- the individual concerned authorizes the second purpose or disclosure;
- non-compliance is necessary to avoid prejudice to
  - the maintenance of the law by any public sector agency (including the prevention, detection, investigation, prosecution, and punishment of offences);
  - the enforcement of a law imposing a pecuniary penalty;
  - the protection of the public revenue;
  - the conduct of proceedings before any court or tribunal; or
- the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained.

Under Section 54, the Privacy Commissioner may also authorize a use and disclosure that would otherwise be inconsistent with PP 10 and PP 11 in circumstances where it is in the public interest or beneficial to the individual, unless the individual has expressly refused to authorize the use and disclosure for that purpose.

Cross-border transfers

PP 11 is silent on cross-border transfers of personal information, and therefore it is implied that cross-border transfers are presumed to be permitted. This is confirmed by Section 114B, which provides that the Privacy Commissioner may prohibit the transfer of personal information from New Zealand to another State if the Privacy Commissioner is reasonably satisfied of two “adequate level of protection” factors:

- the information has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards in the PA; and
- the transfer would be likely to lead to a contravention of the basic principles of national application set out in the OECD Guidelines and set out in Schedule 5A.

However the Privacy Commissioner is unable to prohibit the transfer if the transfer, or the information itself, is required or authorized by or under any enactment; or required by any convention or other instrument imposing international obligations on New Zealand.
Information matching

The PA provides specific protections in relation to provisions between agencies arising from information matching programmes. Under Section 97, an information matching programme is a comparison between documents that contain personal information about 10 or more individuals. The comparison may be conducted either manually or electronically. The comparison must be done for the purpose of producing or verifying information that may be used for the purpose of taking adverse action against an identifiable individual.

The types of permitted information matching provisions are outlined in Schedule 3 of the PA, and relevantly include provisions under the Citizenship Act 1977, Electronic Identity Verification Act 2012, and Immigration Act 2009.

Under Section 99, information must not be disclosed pursuant to an information matching provision unless there is a written agreement between the relevant agencies. The agreement must be forwarded to the Privacy Commissioner. The written agreement must incorporate provisions reflecting the information matching rules as a minimum. The matching rules are detailed in Schedule 4 of the PA, and include requirements for:

- notification to individuals affected;
- limitation on use of unique identifiers to only when it is essential to the success of the programme;
- approval by the Privacy Commissioner of online transfers of information;
- technical standards to govern the operation of the programme;
- safeguards to ensure the validity of discrepancies and results from the matching programme;
- destruction of personal information once no longer required; and
- time limits on the use of a matching programme.

Under Section 100, if the programme produces any “discrepancies,” the relevant agency involved in an authorized information matching programme may take adverse action against an individual.

Under Section 101, the agency must destroy the information containing the discrepancy within 60 working days unless it has taken any adverse action against an individual based on that discrepancy.

Under Section 103, an agency must provide notice to the individual of any adverse action proposed to be taken, the discrepancy on which the adverse action is based, and the minimum 5 working day period in which the individual may respond. Compliance with notification is not required where it would prejudice any investigation into the commission of an offence or the possible commission of an offence.

77 Under Section 97, adverse action means any action that may “adversely affect the rights, benefits, privileges, obligations or interests of any specific individual,” and includes any decision to “to investigate the possible commission of an offence” or “to make a deportation order in relation to the individual, to serve the individual with a deportation liability notice, or to deport the individual from New Zealand.”

78 Presumably a discrepancy arises where the matching programme identifies differences in personal information between two documents about an individual.
Agencies conducting authorized information matching programmes must submit reports to the Privacy Commissioner whenever the Commissioner requires. The Privacy Commissioner must report on certain matters about matching programmes in its annual report. The Privacy Commissioner must also review such agencies and their information matching programmes every 5 years.

**Data quality, access and correction**

Under PP 8, an agency shall not use personal information without taking reasonable steps (if any) to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

Under PP 6, an individual shall be entitled to:

- obtain from the agency confirmation of whether or not the agency holds such personal information; and
- have access to and request correction of that information.

Under PP 7, an agency shall take reasonable steps to correct that information to ensure that the information is accurate, up to date, complete, and not misleading. When deciding on correction, the agency shall have regard to the purposes for which the information may lawfully be used. These steps may be taken by the agency upon its own initiative or upon a request by the individual. If an individual requests a correction, but the agency refuses to make the requested correction, the individual may request that a statement accompany the personal information. This statement will notify that a request for correction had been made. Where steps to correct the information have been made, the agency is to ensure that any recipient of the incorrect information is made aware of the correction.

A right to access personal information concerning other individuals is also provided under the Official Information Act 1982. Disclosure of such personal information may be withheld if disclosure would involve the unwarranted disclosure of the affairs of another person or of a deceased person.

**Retention**

Under PP 9, an agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

**Security**

Under PP 6, an agency shall ensure that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, unauthorized access, use, modification, or disclosure, and other misuse. If it is necessary to give the information to a person relating to a service of the agency, the agency must reasonably ensure that actions are taken to prevent unauthorized use or disclosure of the information.

**Enforcement**

Enforcement under the PA is based upon complaints and investigations conducted by the Privacy Commissioner, which may be settled by conciliation, mediation or referral to the Human Rights Review Tribunal.

---

Pakistan

The right to privacy is implicitly provided for in the Constitution of the Islamic Republic of Pakistan. Article 4 prohibits any action “detrimental to life, liberty, body, reputation or property of any person to be taken except in accordance with the law.” Article 14 provides that the “dignity of man, subject to law, the privacy of home, shall be inviolable.”

While there is no comprehensive federal domestic law relating to privacy and data protection, limited protection is provided in some ordinances. The Electronic Transaction Ordinance 2002 creates an offence relating to unauthorized access to electronic private information.

**Freedom of Information Ordinance 2002**

The Freedom of Information Ordinance 2002 (FOIO) provides for rights to access information held by public bodies subject to certain exemptions under Sections 14-17. The relevant exemptions include:

- records relating to personal privacy of individuals;
- disclosures that would involve the invasion of the privacy of an identifiable individual other than the requester;
- private documents confidentially furnished to a public body;
- any other record excluded by the Federal Government for a public interest reason;
- disclosures that would be likely to cause grave and significant damage to the interests of Pakistan in the conduct of international relations; and
- disclosures that would result in the commission of an offence, harm the detection, prevention, investigation or inquiry in a particular case, reveal the identity of a confidential source of information, facilitate an escape from legal custody, or harm the security of any property or system, including a building, a vehicle, a computer system or communications system.

The Ombudsman may receive complaints under the FOIO and, after conducting investigations, direct that information be disclosed or corrected.
Palau

The right to privacy is implicitly provided for in the Constitution of the Republic of Palau. Section 6 provides that “the government shall take no action to deprive any person of life, liberty, or property without due process of law nor shall private property be taken except for a recognized public use and for just compensation in money or in kind.”

There is no domestic law relating to privacy and data protection.

Papua New Guinea

The right to privacy is expressly provided for in the Constitution of the Independent State of Papua New Guinea. Section 49 guarantees the “right to reasonable privacy in respect of his private and family life, his communications with other persons and his personal papers and effects, except to the extent that the exercise of that right is regulated or restricted by a law that complies with Section 38 (general qualifications on qualified rights).”

Section 51 guarantees the right to freedom of information, providing that “every citizen has the right of reasonable access to official documents” subject only to certain exceptions. Those exceptions relevantly include “national security, defence or international relations,” “papers relating to lawful official activities for investigation and prosecution of crime,” “the prevention, investigation and prosecution of crime,” and “the maintenance of personal privacy and security of the person.”

There is no domestic law relating to privacy and data protection.

---

63 Available at http://www.palauembassy.com/Documents/ConstitutionE.pdf
64 Available at http://www.wipo.int/wipolex/en/text.jsp?file_id=199188
The right to privacy is implicitly provided for in the Constitution of the Republic of the Philippines. Article III on the Bill of Rights provides that "no person shall be deprived of life, liberty or property, the right of people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and the privacy of communication and correspondence."

**Data Privacy Act of 2012**

The Data Privacy Act of 2012 (DPA) is a consolidated privacy law that applies to both the public sector and the private sector. Section 11(a) of the DPA provides the key principle that personal information must be "collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only." The National Privacy Commission (NPC) is the privacy authority, tasked to administer and implement the DPA, and to monitor and ensure compliance with international standards.

**Scope and application**

Under Section 4, the DPA applies to all natural and juridical persons involved in personal information processing, including those who are not physically in the Philippines but use equipment or maintain an office, branch or agency in the Philippines. The DPA therefore applies to government agencies.

Personal information has a broad meaning under Section 3(g). Sensitive personal information is defined under Section 3(l) and attracts additional protections. However, under Section 4, the DPA does not apply to certain pieces of information, including relevantly, "information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by ... law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions." This exemption from the scope of the DPA allows a broad interpretation of what information is “necessary” to carry out the functions of agencies such as law enforcement and immigration agencies. What information is considered “necessary” may still be broadly interpreted. Section 38 of the DPA provides that "any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is process." This provision may limit how broadly “necessary” is interpreted.

---

86 Available at http://www.gov.ph/2012/08/15/republic-act-no-10173/
87 Personal information means “any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.”
88 Sensitive personal information refers to any personal information about “an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by an executive order or an act of Congress to be kept classified.”
Notification

Under Section 16, the data subject is entitled to always be informed that their information will be processed, and be notified of certain details of that processing, including the type of personal information, purpose, scope and method of processing, recipients to whom the information may be disclosed, period of data storage and the existence of their rights to access, correct and lodge a complaint. However, certain exceptions exist which means that only the fact that their information will be processed needs to be notified. Those exceptions arise in several instances, including when the “collection and processing are for obvious purposes” and “when the information is being collected and processed as a result of legal obligation.”

Use and disclosure

Under Section 11(b), personal information will be processed fairly and lawfully. Section 12 elaborates that processing is lawful if not prohibited by law, and where one of several conditions exist. Those conditions relevantly include:

- consent from the individual;
- where processing is necessary for compliance with a legal obligation of the personal information controller;
- where processing is necessary to fulfill functions of a public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; and
- where processing is necessary for the purposes of the legitimate interests of the personal information controller, except where those interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Constitution.

Under Section 13, sensitive personal information can only be processed in certain circumstances, including when there is consent or where the processing concerns personal information that is “necessary … when provided to a government or public authority.”

Disclosure is considered as part of data processing under the DPA. Data controllers have certain requirements relating to disclosure, including security requirements to protect against accidental or unlawful disclosure under Section 20, utilizing contractual or other reasonable means to provide a comparable level of protection while the information is processed by a third party under Section 21, and penalties for malicious disclosure and unauthorized disclosures under Sections 31 and 32.

Cross-border transfers

While there is no separate treatment of cross-border transfers of personal information, it is clear that they are contemplated as part of processing. Under Section 21, personal information controllers are responsible for “information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally.” The requirement under Section 21 to ensure a comparable level of protection from third parties would also arguably apply to cross-border transfers of personal information.

Data quality, access and correction

Under Section 11(c), personal information collected must be “accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date.” Further, “inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.”
Under Section 16, persons are entitled to:

- reasonable access to their personal information;
- dispute the inaccuracy or error of personal information;
- correct, suspend or withdraw their personal information if it is incomplete, outdated, unlawfully obtained, used for unauthorized purposes or is no longer necessary for the purposes for which they were collected; and
- be indemnified for any damages sustained.

Retention

Under Section 11, personal information will be retained only for as long as necessary and kept identifiable for no longer than is necessary for the purposes for which the data were collected and processed. An exception to this arises where it is for historical, statistical or scientific purposes, or where it may be, under law, stored for longer periods.

Security

Section 20 provides for the security of personal information, requiring the personal information controller to implement measures to protect against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. This includes natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. Section 20(c) outlines the requirements for the security measures, including security policies, processes for vulnerability assessment in computer networks, and regular monitoring for security breaches.

Under Section 20(f), personal information controllers are required to notify the NPC and affected data subjects when personal information is acquired by an unauthorized person and where it is likely to give rise to a real risk of serious harm to any affected data subject. Notification may be exempted if notification would not be in the public interest or in the interests of affected data subjects. It may be postponed if it hinders progress of a criminal investigation related to a serious breach.

Chapter VII provides additional principles regarding data security of sensitive personal information within government. These include responsibility by the head of each government agency for complying with security requirements, and that government workers will only have access to sensitive personal information if they have a security clearance.

Accountability

Section 21 provides that each personal information controller is responsible for personal information under its control or custody. The personal information controller is accountable for complying with the requirements of the Act, and for utilizing means to provide a comparable level of protection while the information is processed by a third party. The personal information controller can also designate other individuals to be similarly accountable.
Enforcement

The NPC’s functions include receiving complaints, instituting investigations, imposing temporary or permanent bans on the processing of personal information if such processing will be detrimental to national security and public interest, coordinate with other government agencies and the private sector on efforts to formulate and implement privacy plans and policies; propose legislation, amendments or modifications to laws on privacy or data protection, and facilitate cross-border enforcement of data protection.

The NPC may also recommend to the Department of Justice the prosecution and imposition of penalties specified in the DPA. Under Sections 25-20, these penalties relate to unauthorized processing, accessing personal information due to negligence, improper disposal, processing for unauthorized purposes, and unauthorized access or intentional breach. The NPC cannot provide recommendations in relation to penalties under Sections 30-32, which include concealment of security breaches, malicious disclosure, and unauthorized disclosure. All these offences include both monetary and imprisonment penalties.

When a public officer commits any of these offences, the public officer may also be disqualified from occupying public office for a term that is double the imprisonment term imposed.
Republic of Korea

The right to privacy is expressly provided for in the Constitution of the Republic of Korea. Article 17 provides for the inviolable right to enjoy privacy and that each individual has right to control and determine their own personal information.

Personal Information Protection Act 2011

The Personal Information Protection Act 2011 (PIPA) is a comprehensive privacy law that provides for the “processing of the personal information for the purpose of enhancing the right and interest of citizens, and further realizing the dignity and value of the individuals by protecting their privacy from the unauthorized collection, leak, abuse or misuse of personal information.” Privacy protection within the PIPA is primarily based around Personal Information Protection Principles (PIPPs) as outlined in Article 3 of the PIPA.

The Personal Information Protection Commission (PIPC), consisting of up to 15 commissioners, is the primary privacy authority.

Scope and application

The PIPA applies to “public institutions,” which includes administrative bodies of the parliament, judicial and electoral commission, and the central administrative departments and agencies, their affiliated bodies, and local governments.

Notification and collection

The first PIPP provides that the “personal information processor shall make the personal information processing purposes explicit and specified, and shall collect minimum personal information lawfully and fairly to the extent necessary for such purposes.”

Under Article 4, the data subject has the right to be informed of the processing of their personal information, the right to consent or not consent and to elect the scope for the consent.

Under Article 15, personal information processors can collect personal information only in some certain circumstances, including relevantly where:

- consent is obtained from data subjects;
- special provisions exist in laws or it is unavoidable so as to observe legal obligations;
- it is unavoidable so that the public institution may carry out such work under its jurisdiction as stated by laws and regulations; or
- it is necessary to attain the justifiable interest of personal information processor, which is explicitly superior to that of data subjects. In this case, it is allowed only when substantial relation exists with the justifiable interest of personal information processor and it does not go beyond the reasonable scope.

Available at http://www.koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf
Where consent is obtained, data subjects are to be informed of the purpose of collection and use, what personal information is being collected, the retention period, and the fact that data subjects are entitled to deny consent, and the disadvantage affected from the denial of consent.

Under Article 16, the personal information processor shall collect only the minimum personal information necessary for the purpose of collection. The personal information processor shall not deny goods or services on the ground that they will not consent to collection of personal information exceeding this minimum requirement.

Use and disclosure

The second PIPP provides that the “personal information processor shall process personal information compatibly to the extent necessary to attain the personal information processing purposes, and shall not use beyond such purposes.”

The sixth PIPP provides that the “personal information processor shall process personal information in a manner to minimize the possibility to infringe upon the privacy of data subject.”

The seventh PIPP provides that the “personal information processor shall make efforts to process personal information in anonymity, if possible.”

Under Article 23, a personal information processor will not process sensitive information without the data subject’s consent or where laws and regulations require, or permit, the processing of sensitive information.

Under Article 17, the personal information processor may provide or share personal information to a third party in certain circumstances, which relevantly include where:

- the consent is obtained from data subjects; or
- personal information is provided within the scope of purposes for which personal information is collected for various purposes, including relevantly, observing legal obligations or for a public institution to carry out work under its jurisdiction as stated by laws and regulations.

When consent is required to provide information to a third party, the personal information processor is required to notify the data subject of the recipient third party, the purpose of the third party’s use of the personal information, what personal information is being provided, and retention period, and that data subjects can deny consent.

Under Article 18, the personal information processor shall not use or disclose personal information beyond the scope allowed upon collection. However, some exceptions apply, including relevantly where:

- there is additional consent from the data subject;
- it is otherwise impossible to carry out the work of the personal information processor’s lawful jurisdiction (subject to the deliberation and resolution of the PIPC);
- it is necessary to provide personal information to a foreign government or international organization so as to perform a treaty or other international convention; or
- it is necessary for the investigation of crimes, indictment and prosecution.

91 Information relating to “ideology, belief, admission/exit to and from trade unions or political parties, political mindset, health, sexual life, and other personal information which is likely doing harm to privacy of data subjects.”
If the above circumstances apply (other than obtaining additional consent and for the investigation of crimes), the public institution is to publish in the official gazette or its public website the legal grounds for such disclosure.

Where information is provided to a third party, the personal information processor shall request the recipient of personal information to restrict the purpose and method of use and other necessary matters, or to prepare for necessary safeguards to ensure the safety of personal information.

Under Article 19, the person who receives personal information from the personal information processor shall not use personal information for other purpose than the intended one, or shall not provide it to a third party except where additional consent is obtained from data subjects or special provisions exist in other laws.

Cross-border transfers

Cross-border transfers of personal information are treated substantially in the same way as domestic disclosures. Under Article 17(3), when there is a provision of personal information overseas, the personal information processor must obtain the data subject’s consent and notify them of the third party recipient, the purpose of the third party’s use of the personal information, what personal information is being provided, and retention period, and that data subjects can refuse to provide consent. However, the exceptions under Article 18 above also apply to Article 17(3).

Under Article 14(2), the government is required to establish “policy measures so that the rights of data subjects may not be infringed upon owing to cross border transfer of personal information.”

Security

The fourth PIPP provides that the “personal information processor shall manage personal information in a safe way according to the personal information processing methods, types, etc. in consideration of the possibility that the data subject rights are infringed upon and the degree of such risks.”

Article 5 requires governments to devise policies to prevent harmful consequences of beyond purpose collection, abuse and misuse of personal information.

Article 29 requires the personal information processor to take such “technical, managerial and physical measures as internal management plan and preservation of log-on records etc. necessary to ensure the safety so that personal information may not be lost, stolen, leaked, altered or damaged.”

Under Article 33, public institutions are required to conduct “the assessment for the analysis and improvement or risk factors” (a privacy impact assessment), “in case of probable violation of personal information of data subjects owing to the operation of personal information files.”

Data quality, access and correction

The third PIPP provides that the “personal information processor shall ensure the personal information is accurate, complete and up to date to the extent necessary to attain the personal information processing purposes.”
The fifth PIPP provides that the “personal information processor shall make public its privacy policy and other personal information processing matters, and shall guarantee the data subject rights including the right to access to his/her personal information.”

Under Article 4(3), the data subject has the right to demand access to personal information, suspend processing, and seek to correct, delete and destroy personal information. The procedure for these rights is established in Articles 35 and 36. Relevantly, under Article 35(4), access may be restricted or prohibited by law. Under Article 37, a data subject may demand the personal information processor to suspend the processing of his or her own personal information.

Individuals also have general access rights under the Act on Disclosure of Information by Public Agencies 1996. However, certain relevant exceptions exist to disclosure of information, including:

- maintained as secrets or provided as non-disclosable by other laws, decrees or ordinances;
- which could harm major national interests in such fields as national security, national defense, unification or diplomatic relations if disclosed;
- which could substantially harm the lives, bodies and properties of the people, and other public safety or interests if disclosed;
- related to the prevention and investigation of crimes, institution and maintenance of public prosecution, execution of sentences, correction, security measures, and pending litigation;
- which could substantially hamper the performance of duties or violate the criminal defendant’s right to a fair trial if disclosed;
- related to internal processes which could substantially hamper the fair performance of duties, studies and development if disclosed; or
- that is personal information which could identify a particular individual, except for personal information:
  - which is available for public inspection in accordance with legislation;
  - drawn up or obtained by the public agencies which is subject to public notification; and
  - drawn up or obtained by the public agencies disclosure of which is necessary in order to remedy public interests or private rights.

Retention

Under Article 21, the personal information processor shall destroy the personal information without delay when such personal information becomes unnecessary owing to the expiry of retention period, attainment of purpose of personal information processing. However, an exception arises where preservation of the personal information is mandatory by other laws and regulations.

Accountability

The eighth PIPP provides that the “personal information processor shall make efforts to obtain trust of data subjects by observing and carrying out such duties and responsibilities as stated in this Act and other related laws and regulations.”

Available at http://www.freedominfo.org/documents/korea%20980258118__korea.doc
Article 5 requires governments to devise policies and work out policy measures relating to the protection of privacy. Article 9 requires the Minister of Public Administration and Security to establish a Data Protection Basic Plan with every head of central administrative department and agency. Under Article 10, the head of the department or agency is to establish an implementation plan in accordance with the Basic Plan. Under Article 12, the Minister of Public Administration and Security and the head of the department or agencies have the discretion to establish standard data protection guidelines.

Under Article 28, the personal information processor must conduct appropriate control and supervision of officers and employees (personal information handler) and provide necessary education programs to ensure appropriate handling of personal information.

Under Article 31, a personal information processor shall designate a privacy officer who comprehensively takes charge of personal information processing.

**Enforcement**

Under Article 8, the PIPC is tasked to deliberate and resolve the various matters regarding data protection, including improvement of policies, systems and legislation related with data protection, and the interpretation and operation of laws and regulations related with data protection.

Under Article 4(5), the data subject has the right to appropriate redress for any damage arising out of the processing of personal information in a prompt and fair procedure. Under Article 39, any data subject who suffers damage caused by a violation of the PIPA may claim damages against the personal information processor.

Under Article 64, the Minister of Public Administration and Security and heads of central administrative departments or agencies may order relevant corrective measures where they consider there is an infringement of the PIPA and it left unattended, the infringement will likely cause irreparable injury. The measures include suspending any violation of personal information, temporarily suspending processing, and any other necessary measures for the protection of, or prevention of infringement upon, personal information.

Chapter IX provides penalties for various offences, including for violations of the consent, processing, disclosure, and security provisions of the PIPA. There is an additional penalty for causing the “suspension, paralysis or other severe hardship of work of public institutions by altering or deleting the personal information processed by the said institutions.”
Samoa

The right to privacy is implicitly provided for in the Constitution of the Independent State of Samoa.\textsuperscript{33} Article 6 guarantees that “no person shall be deprived of his personal liberty except in accordance with law.”

There is no domestic law relating to privacy and data protection.

Singapore

The Constitution of the Republic of Singapore does not expressly provide any privacy or privacy related rights.\textsuperscript{34}

Personal Data Protection Act 2012

The Personal Data Protection Act 2012 (PDPA)\textsuperscript{95} is a comprehensive privacy law that aims to “govern the collection, use and disclosure of personal data by organizations in a manner that recognizes both the right of individuals to protect their personal data and the need of organizations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.” The Personal Data Protection Commission (PDPC) is the privacy authority.

Scope and application

The PDPA applies to “personal data,” which is data, whether true or not, about an individual who can be identified from that data or from that data and other information to which the organization has or is likely to have access. An individual is “a natural person, whether living or deceased.” This appears to include non-nationals as well.

The PDPA applies to organizations, which include “any individual, company, association or body of persons, corporate or unincorporated.” This arguably includes a “public agency,” which includes the “government, including any ministry, department, agency or organ of State.”

Significantly, under Section 4, the provisions relating to the collection, use and disclosure of personal data does not apply to a public agency. This means that the government, including law enforcement and immigration agencies, has a complete exemption under the PDPA in relation to the collection, use and disclosure of personal data.

\textsuperscript{33} Available at http://www.samlii.org/ws/legis/consol_act/cotisos1960438/
\textsuperscript{34} Available at http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%22cf2412ff-fca5-4a64-a8ef-b95b8987728e%22%20Status%3AINforce%20Depth%3A0;rec=0
\textsuperscript{95} Available at http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3AINforce;rec=0
Cross-border transfers

While public agencies are generally exempt from provisions relating to disclosure of personal data, they are not exempt from cross-border transfer of personal information protections. Under Section 26, any organization, including a public agency, cannot transfer personal data to a country or territory outside of Singapore unless the same requirements under the PDPA are met to ensure that organizations provide a standard of protection to personal data that is comparable to the PDPA. The PDPC may exempt an organization from this requirement.

Data quality, access and correction

Under Section 23, if personal data will be used to make a decision affecting the individual, or is likely to be disclosed, a public agency must make reasonable effort to ensure that personal data collected is accurate and complete.

Under Section 21, upon a request from the individual, a public agency must provide them with the personal data about them in the public agency’s possession. The public agency must inform them of how the data may have been used or disclosed in the year prior to the request. Certain categories of information are exempt from this section, including any personal data collected for the purpose of an investigation if the investigation and associated proceedings and appeals have not been completed. The definition of an investigation is broad and includes “an investigation relating to a contravention of any written law or … any other requirement imposed by any regulatory authority in exercise of its powers under any written law.”

Further, a public agency may choose to not provide information in some circumstances. These circumstances include where it might cause harm to another individual or grave harm to the individual, reveal personal data of another individual, or is contrary to the national interest.

Under Section 22, an individual may request to correct an error or omission in the personal data held about them. The personal data will be corrected as soon as possible and the correction notified to other organizations to which that personal data has been disclosed within the year before the correction was made. A broad exception to this requirement exists where the public agency is satisfied on reasonable grounds that the correction should not be made.

Certain categories of information are exempt from this section, including any personal data or document related to a prosecution if all proceedings related to the prosecution have not been completed.

Retention

Under Section 25, a public agency must cease to retain documents containing personal data, or de-identify the data, when it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the data. Retention must also no longer be necessary for legal or business purposes.

Security

Under Section 24, a public agency must protect personal data by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.
Enforcement

Under Section 50, the PDPC may, upon complaint being lodged or its own motion, conduct an investigation into whether an organization is complying with the PDPA. The PDPC may also refer complaints for mediation, review decisions relating to refusal to provide access to or correct personal data. Under Section 30, the PDPC may give directions as it thinks fit in the circumstances to ensure compliance. These directions may include that an organization stop collecting, using or disclosing personal data in contravention of the PDPA, destroy personal data collected in contravention of the PDPA, and to pay a financial penalty. These directions can be registered and enforced in the District Court.

Under Section 32, an individual who suffers loss or damage as a result of a contravention of the PDPA shall have the right of action for relief in civil court proceedings. Such relief may be by way of injunction or declaration, damages, or such other relief as the court thinks fit.

Under Sections 51 and 52, various offences exist for non-compliance with the PDPA, including obtaining access or changing personal data about another individual without the authority of that individual, obstructs or impedes the PDPC in its duties and functions.

Solomon Islands

The right to privacy is implicitly provided for in the Constitution of the Solomon Islands. Article 9 protects the privacy of home and other property. It provides that “except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises.” Article 9 also provides that any act contained in or done under the authority of certain laws is deemed to be not inconsistent with this provision. Those laws must make provision in relation to various purposes, for example, the interests of “defence, public safety, public order, the prevention and investigation of breaches of the law, public morality, public health,” “protecting the rights or freedoms of other persons,” and “entry upon any premises for the purpose of preventing or detecting criminal offences.”

There is no domestic law relating to privacy and data protection.

96 Available at http://www.wipo.int/wipolex/en/text.jsp?file_id=198229
Sri Lanka

The right to privacy is not explicitly enshrined in the *Constitution of the Democratic Socialist Republic of Sri Lanka.*

While there is no comprehensive domestic law relating to privacy and data protection in Sri Lanka, as part of the Government’s 2010 Policy and Procedures of ICT Usage in Government, the government has been pursuing the adoption of a Data Protection Code of Practice, with the possibility of the code being placed on a statutory footing through regulations issued under the *Information and Communication Technology Act of 2003.*

Syria

The right to privacy is implicitly provided for in the *Syrian Arab Republic: Constitution.* Article 36 guarantees that the “inviolability of private life shall be protected by the law” and that “houses shall not be entered or inspected except by an order of the competent judicial authority in the cases prescribed by law.” Article 37 guarantees the “confidentiality of postal correspondence, telecommunications and radio and other communication shall be guaranteed in accordance with the law.”

There is no domestic law relating to privacy and data protection.

---

99 Available at http://www.unhcr.org/refworld/docid/5100f02a2.html
Thailand

The Constitution of Thailand is presently under drafting and development. Under the 2007
*Constitution of the Kingdom of Thailand,* the right to privacy was implicitly provided for in Article 35, which provided that “person’s family rights, dignity, reputation and the right of privacy shall be
protected. The assertion or circulation of a statement or picture in any manner whatsoever to the
public, which violates or affects a person’s family rights, dignity, reputation or the right of privacy, shall
not be made except for the case which is beneficial to the public. Personal data of a person shall be
protected from the seeking of unlawful benefit as provided by the law.”

**Official Information Act 1997**

The *Official Information Act 1997* (OIA), in addition to establishing an access to information
framework, also establishes privacy protections that apply specifically to government agencies. The
primary privacy authority is the Official Information Board (OIB). The functions of the OIB include
advising on the implementation of the OIA, giving recommendations on Royal Decrees, Ministerial
Regulations and other rules, and receiving complaints. The OIB website provides general information,
as well as documents regarding discussions and consultations regarding personal information.

**Scope and application**

Personal information has a broad meaning under Section 4 of the OIA. Under the privacy provisions
in Chapter 3, the rights and privileges established are limited to persons who are either Thai nationals
or those who reside in Thailand. Migrants and travelers within Thailand who do not reside in Thailand
are not covered by the OIA. The OIA specifically applies to State agencies.

**Collection and notification**

Under Section 23, any personal information system will be provided only where it is relevant and
necessary to the objectives of the State agency, and will be terminated when it is no longer necessary.
State agencies are to make efforts to collect information directly from the person the subject of the
information.

The collection of personal information will be published in a Government Gazette, notifying the public
of various basic details of collection. However, security agencies do not need to comply with this
requirement.

---

100 Available at [http://www.constitutionalcourt.or.th/dmdocuments/Constitution2007byIFES.pdf](http://www.constitutionalcourt.or.th/dmdocuments/Constitution2007byIFES.pdf)
103 Personal information means “an information relating to all the personal particulars of a person, such as education, financial status, health record, criminal record or employment record, which contain the name of such person or contain a numeric reference, code or such other indications identifying that person as fingerprint, tape or diskette in which a person’s sound is recorded, or photograph, and shall also include information relating to personal particulars of the deceased.”
104 State agencies mean “a central administration, provincial administration, local administration, State enterprise, Government agency attached to the National Assembly, Court only in respect of the affairs unassociated with the trial and adjudication of cases, professional supervisory organisation, independent agency of the State and such other agency as prescribed in the Ministerial Regulation.”
105 Undefined under the OIA
When information is collected directly from the person, the State agency shall notify the person of the purpose for the use of the information, the ordinary nature of its use, and whether the collection is voluntary or compulsory.

If the personal information is “dispatched to any place” that might result in it being publicly known and this is outside the ordinary use of the information, the State agency will notify the person concerned.

**Use and disclosure**

There is no explicit requirement for personal information to only be used for the purposes notified to the person. While State agencies are required to notify about the “ordinary use” of the personal information, the limitation on the use of a personal information system appears to only relate to its “relevance and necessity” to the objectives of the State agency.

Under Section 24, a State agency can only disclose personal information to another State agency or other “persons” if there is prior or immediate written consent from the individual concerned unless disclosure occurs in certain circumstances. Those exceptional circumstances relevantly include:

- disclosures within the ordinary use within the objections of the provision of the personal information system;
- preventing violation of law or non-compliance with the law;
- conducting investigations and inquiries (to other State agencies only), under compulsion of the law; and
- any other case prescribed by Royal Decree.

**Cross-border transfer**

The provisions of the OIA do not appear to regulate cross-border transfers of personal information. Disclosures authorized under Section 24 only apply to disclosures to other State agencies and other persons. “Persons” in this chapter means “a natural person who is of Thai nationality and a natural person who is not of Thai nationality but has a residence in Thailand.” This definition may include diplomats and foreign officials who are residents of Thailand, but would not involve foreign officials who do not live in Thailand.

**Access and correction**

Under Section 25, persons have the right to access and to make a request to correct, alter or delete any incorrect information. In relation to access to information, a State agency may prohibit the disclosure of information for various reasons under Sections 14 and 15, including that the “disclosure thereof will result in the decline in the efficiency of law enforcement or failure to achieve its objectives, whether or not it is related to litigation, protection, suppression, verification, inspection, or knowledge of the source of the information.” A person may appeal to the Information Disclosure Tribunal within 15 days.

If after a request for correction, a state agency decides to not correct, alter or delete the information, the person has a right to appeal to the Information Disclosure Tribunal within 30 days of the decision notification.
Retention

There are no provisions relating to retention of specific or individual pieces of personal information. More broadly, under Section 23(1), personal information systems are required to be terminated when it is no longer necessary for the achievement of the objectives of the operation of the State agency.

Security

Under Section 23(5), an appropriate security system will be provided to prevent “improper use or any use to the prejudice of the person who is the subject of the information.”

Enforcement

Under Section 32, the OIB shall have the power to summon any person to give statements or to furnish an object, document or evidence for its consideration. Failure to comply with such a summon incurs a penalty of imprisonment or a fine.

Timor-Leste

The right to privacy is expressly provided for in the Constitution of the Democratic Republic of Timor-Leste. Section 36 guarantees the individual’s “right to honour, good name and reputation, protection of his or her public image and privacy of his or her personal and family life.” Section 37 provides that “any person’s home and the privacy of his or her correspondence and other means of private communication are inviolable except in cases provided for by law as a result of criminal proceedings.”

Section 38 guarantees the protection of personal data. It provides every citizen with the “right to access personal data stored in a computer system or entered into mechanical or manual records regarding him or her, and he or she shall have the right to demand the purpose of such data.” Section 38 also requires the law to determine “the concept of personal data, as well as the conditions applicable to the processing thereof” and that the processing of personal data on private life and other types of information is prohibited unless there is consent from the interested person.

There is no domestic law relating to privacy and data protection.

Tonga

The right to privacy is implicitly provided for in the Constitution of Tonga.\textsuperscript{107} Article 16 guarantees the right against the forcible entry of “houses or premises of another or to search for anything or to take the property of another except according to law.”

There is no domestic law relating to privacy and data protection.

Turkey

The right to privacy is expressly provided for in the Constitution of the Republic of Turkey.\textsuperscript{108} Article 20 provides that everyone is entitled to the protection of their personal data. Such protection includes the right to be informed about their personal data, and to access the data and request correction or destruction of such data. Personal data may only be processed with the explicit consent of the relevant person or as envisaged by law. It is further stipulated that the principles and procedures regarding the use of personal data are to be regulated by legislation to that effect.

While no comprehensive privacy law has been enacted, privacy and confidentiality are protected in various separate codes and laws. Under Article 23 of the Civil Code (Law No: 4721),\textsuperscript{109} no person may waive his/her freedoms or have such freedoms limited in a manner contrary to law or morality. Article 24 further states that a person whose “personality right” has been violated may request protection from such violation from the court. Each violation of an individual’s personality right is deemed to be illegal unless the consent of the subject person is obtained or there is a higher degree of private or public benefit, or occurs via a statutory authority.

Under the Law on the Right to Information (Law No: 4982 of 2003),\textsuperscript{110} individuals are provided with the right to access the information held about them by public institutions. There is no explicit right to correct information. The right to access information is subject to certain general restrictions, including information or documents that, under Articles 19-22:

- relate to administrative investigations that clearly violate the right of privacy of individuals or that jeopardize the security of the investigation, or would disclose the source of the information that needs to be kept secret;
- endanger the prevention and investigation of a crime, or endanger the legal procedure for the detention and prosecution of criminals;
- unjustly interfere with health records, private and family life, honour and dignity, and economic and professional interests of an individual, unless there is consent of the individual; or
- violate the privacy of communication.

\textsuperscript{107} Available at http://www.wipo.int/wipolex/en/text.jsp?file_id=200829
\textsuperscript{108} Available at http://global.tbmm.gov.tr/docs/constitution_en.pdf
\textsuperscript{109} Available at http://www.justice.gov.tr/basiclaws/turkish_civil.pdf
\textsuperscript{110} Available at http://www.refworld.org/docid/4c4475812.html

Privacy and data protection laws of Bali Process member States
The right to privacy is implicitly provided for in the Constitution of the United Arab Emirates. Article 31 provides for “freedom of communication by means of the posts, telegraph or other means of communication and their secrecy shall be guaranteed in accordance with the law.” Article 36 provides that “homes shall be inviolable. They may not be entered without permission from their inhabitants except in accordance with the provisions of the law, and in circumstances laid down therein.”

There is no general consolidated privacy law that applies to the whole of the UAE.

**Dubai International Financial Center – Data Protection Law of 2007**

A comprehensive privacy law has been enacted that applies within the Dubai International Financial Center – the *Data Protection Law of 2007* (DPL). The DPL aims to “to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.”

The Commissioner of Data Protection (CDP) is the privacy authority, and is empowered with powers, duties and functions in the pursuit of the objectives of the DPL.

**Application**

Personal data refers to any identifiable natural person. An identifiable natural person is any natural living person who can be identified, directly or indirectly, by reference to an ID number or other factors including their biological, physical, biometric, physiological, mental, economic, cultural or social identity.

Sensitive Personal Data is any personal data that relates to racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life.

The application of the privacy protection applies to Data Controllers and Data Processors, which includes a government or state under Paragraph 1(1)(b) of Schedule 1.

**Notification**

Under Section 13, data controllers are required to provide a data subject with certain information, including the identity of the data controller, the purposes of processing, and any other further information which is necessary to guarantee fair processing. Data controllers are required to provide this information as soon as possible upon commencing to collect the personal data. Data controllers are not required to provide this notification if they reasonably expect that the data subject is already aware of that information.

111 Available at http://uaecabinet.ae/en/UAEGovernment/Pages/UAE-Constitution.aspx
112 Available at https://www.difc.ae/sites/default/files/dp-law.pdf
Under Section 14, if personal data is not collected directly from the data subject, notification must occur not later than when it is first processed or disclosed. This is not required if data controllers reasonably expect that the data subject is already aware of that information, or that notification is impossible or would involve a disproportionate effort.

**Use and disclosure**

Under Section 8(1), personal data must be “processed fairly, lawfully, and securely,” and “processed for specified, explicit and legitimate purposes in accordance with the data subject’s rights and not further Processed in a way incompatible with those purposes or rights.”

Under Section 9, personal data can only be processed in certain circumstances, including if there is written consent from the data subject, or relevantly where processing is necessary for:

- compliance with any legal obligation to which the data controller is subject; and
- the legitimate interests pursued by the data controller, or by the third party or parties to whom the personal data is disclosed, unless such interests are overridden by compelling legitimate interests of the data subject.

Under Section 10, sensitive personal data can only be processed in certain circumstances. Those exceptions circumstances arise if there is written consent from the data subject, or relevantly where processing is necessary for:

- purposes of carrying out the obligations and specific rights of the data controller;
- compliance with any regulatory or legal obligation to which the data controller is subject; or
- compliance with any regulatory requirements or the prevention or detection of any crime that apply to a data controller.

These protections do not apply if a permit has been obtained from the CDP and the data controller applies adequate safeguards in relation to the processing of sensitive personal data.

**Cross-border transfer**

Under Article 11, a cross-border transfer of personal information can occur if there receiving jurisdiction is listed as having an adequate level of protection as approved by the CDP. Under Article 12, personal data may be transferred to a jurisdiction without an adequate level of protection if:

- there is a permit from the CDP;
- there is written consent from the data subject about the proposed transfer; or
- the transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defence of legal claims.

**Security**

Under Article 16, the data controller must implement appropriate technical and organizational measures to protect personal data against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.

---

113 The list of adequate data protection regimes/centers can be found at https://www.difc.ae/adequate-data-protection-regimes. The Bali Process member States included in this list are New Zealand and the United States, under the US Department of Commerce Safe Harbor Policy.
If there is processing carried out by a data processor, the data controller shall choose a data processor that provides sufficient guarantees on technical security and organizational measures governing the processing to be carried out. The data controller shall ensure compliance with those measures.

Where there is an unauthorized intrusion, either physical, electronic or otherwise, to any personal data database, the data controller or processor carrying out the data controller’s function at the time of the intrusion, shall inform the CDP of the incident as soon as reasonably practicable.

Data quality, access and correction

Under Article 8(1), processed personal data must be “adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed” and “accurate, and where necessary, kept up to date.”

Under Article 8(2), data controllers must take “every reasonable step … to ensure that personal data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified.”

Under Article 17, a data subject has the right to request and obtain from the data controller:

- written confirmation on whether or not personal data relating to him is being processed;
- information about the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data are disclosed;
- information about the personal data being processed and its source; and
- as appropriate, the rectification, erasure or blocking of personal data which does not comply with the DPL.

Retention

Under Article 8(1)(e), personal data must be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was collected or for which they are further processed.”

Enforcement

Under Article 26, the CDP’s powers include issuing warnings and recommendations to data controllers, initiating legal proceedings for contraventions of the DPL, imposing fines for non-compliance, initiating claims for compensation on behalf of the data subject, and submitting draft regulations, standards and codes of practice regarding the DPL. Data subjects can lodge complaints with the CDP under Article 34. Contraventions of the DPL result in maximum fines as outlined in Schedule 2 of the DPL.
United States of America

The right to privacy is implicitly provided for in the Fourth Amendment of the Constitution of the United States of America, which protects against unreasonable searches and seizures. The United States does not have a comprehensive data protection law, but instead regulates primarily on a sector-by-sector basis.

Privacy Act of 1974

The Privacy Act of 1974 (5 U.S.C. § 552a) (PA) is the law that regulates government agencies. Under Section 552(v), the Director of the Office of Management and Budget is the privacy authority and has overall responsibility to develop and prescribe relevant guidelines and regulations, and provide continuing assistance to and oversight of agencies’ implementation of the PA.

Scope and application

Under Section 552(a), the PA applies to US citizens and aliens with permanent residence. The PA applies to “systems of records,” which means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol or in part in making any determination about an identifying individual. A “record” is “any item, collection, or grouping of information about an individual that is maintained by an agency.”

Under Section 552(j) and (k), heads of agencies may establish rules for exempting various agency requirements under the PA as it relates to intelligence and criminal law enforcement activities.

Notification and collection

Under Section 552(e), each agency shall maintain in its records only such personal information as is relevant and necessary to accomplish a purpose of the agency. The agency may only collect information to the greatest extent practicable directly from the individual when that information may result in adverse determinations about the individual’s rights, benefits and privileges under federal programs.

Under Section 552(e)(3), the agency must inform each individual about the legal authority which authorizes collection of the personal information, and whether that is mandatory or voluntary; the purpose for which the information is intended to be used, the routine uses of the information, and the effects of not providing all or part of the information.

Under Section 552(e)(4), the agency must publish a notice of the Federal Register the existence and character of the system of records. The notice is to include, among other things, the name and location of the system, the categories of the individuals whose records will be maintained in the system, the categories of records maintained in the system, the routine uses, agencies’ policies and practices regarding storage, retrievability, access controls, retention and disposal of records.

114 Available at http://www.archives.gov/exhibits/charters/constitution.html
Use and Disclosure

Under Section 552(e)(1), an agency may only maintain records of information about an individual as is relevant and necessary to accomplish a purpose of the agency, as required under statute or executive order. Agencies may only use records of information for routine uses, which are the “the use of such record for a purpose which is compatible with the purpose for which it was collected.”

Under Section 552(b), no agency shall disclose any record which is contained in a system of records except where there is a written request or written consent by the individual, or in certain exceptional circumstances. Those exceptional circumstances relevantly include disclosures:

- to officers within the agency who require the record in performing of their duties;
- required under the PA;
- for a routine use and described under a public notice in the Federal Register;
- for a civil or criminal law enforcement activity, and where the head of the agency has made a written request specifying the record requested and the enforcement activity; and
- pursuant to the order of a court or competent jurisdiction.

Under Section 552(c), agencies are required to keep records of disclosures for at least 5 years or the life of the record.

Matching programs

The PA also provides protections in relation to government use of computer matching programs. Under Section 552(p), every agency that participates in a matching program must establish a Data Integrity Board (DIB) to oversee and coordinate the implementation of the provisions under the PA.

Under Section 552(o), records may not be disclosed to another agency (including a non-federal agency) for the purposes of a matching program except under a written agreement between the two agencies. The matching agreement must state:

- the purpose and legal authority for conducting the matching program;
- the justification for the program and its anticipated results, including an estimate of any savings;
- a description of the records that will be matched, including each data element used, the approximate number of records to be matched, and the projected starting and completion dates of the matching program;
- procedures for notifying individuals and the DIB, verifying the information produced under the matching program, and retention, security, and use of the information produced;
- any assessments of the accuracy of the records used; and
- that the Comptroller General may access all of the records deemed necessary in order to monitor compliance with the agreement.

The matching agreement must be provided to the Senate Committee on Governmental Affairs and the House Committee on Government Operations, and made available to the public. The DIB may determine the term of the agreement, with the maximum term being 18 months. However, the DIB may also renew a matching agreement for a further year if no changes are made to the agreement and each agency certifies that there has been compliance with the agreement. If the DIB does not approve a proposed matching agreement, either party agency may appeal to the Director of the Office of Management and Budget.

 Defined as “computerized comparison of databases in order to determine the status, rights, or benefits of the individuals within those systems of records”
Security

Under Section 552(e)(10), agencies must establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Data quality, access and correction

Under Section 552(e)(5), an agency must maintain all records which are used by the agency with such accuracy, relevance, timeliness, and completeness as reasonably necessary to ensure fairness to the individual.

Under Section 552(e)(6), the agency must make reasonable efforts to assure that the records are accurate, complete, timely and relevant prior to dissemination to any person outside of the agency.

Under Section 552(d), each agency, upon a request by any individual for their information, shall allow the individual access to review and copy the personal information, and to request amendments of the record. The agency may then make any correction requested by the individual regarding accuracy, relevance, timeliness or completeness of the record, or otherwise inform the individual of its refusal to amend the record and the reason for the refusal. The individual has the right to review within 30 days.

Under Section 552(f), each agency is to establish procedures for this request, access, correction or refusal process. Similar rights are also provided under the Freedom of Information Act 1967 (5 U.S.C. § 552) subject to certain exceptions. These exceptions relevantly relate to information that:

- is classified to protect national security;
- related solely to the internal personnel rules and practices of an agency;
- is prohibited from disclosure by another federal law;
- concerns communications within or between agencies which are protected by legal privileges;
- if disclosed, would invade another individual’s personal privacy; or
- is compiled for law enforcement purposes and it:
  - could reasonably be expected to interfere with enforcement proceedings;
  - would deprive a person of a right to a fair trial or an impartial adjudication;
  - could reasonably be expected to constitute an unwarranted invasion of personal privacy;
  - could reasonably be expected to disclose the identity of a confidential source;
  - would disclose techniques and procedures for law enforcement investigations or prosecutions; or
  - could reasonably be expected to endanger the life or physical safety of any individual.

Retention

Under Section 552(e)(1), an agency may only maintain records of information about an individual as is relevant and necessary to accomplish a purpose of the agency, as required under statute or executive order. This implies a requirement that the agency cease to maintain records where it is no longer relevant or necessary to a purpose of the agency.

Accountability

Under Section 552(e)(9), an agency must establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance.

Enforcement

Under Section 552(g), if there is a failure to comply with the provisions of the PA that has an adverse effect on an individual, the individual affected may bring a civil action against the agency.

Under Section 552(i), criminal penalties may be imposed on officers of an agency for prohibited disclosure by an officer of an agency, failure to meet public register notice requirements, and collection of personal information under false pretenses.
Vanuatu

The right to privacy is expressly provided for in the Constitution of the Republic of Vanuatu. Article 5 protects the rights of individuals to “life, liberty… [and] protection for the privacy of the home and other property and from unjust deprivation of property,” subject to respect for the rights and freedoms of others and “to the legitimate public interest in defence, safety, public order, welfare and health.”

While there is no comprehensive law relating to privacy and data protection, some data protection provisions exist under the Electronic Transactions Act 2000 (ETA).

Under Section 25 of the ETA, the Minister may make orders prescribing standards for the processing of personal data, whether or not the personal data originates inside Vanuatu. Such regulations may relate to:

- the voluntary registration to the standards by data controllers and data processors;
- the establishment of a public register showing particulars of data controllers and data processors registered to these standards, the dates of registration, and the countries in respect of which the registration applies;
- the application of the standards to those countries specified in the regulations; and
- different standards applicable to personal data originating from different countries.

To date, no such regulations have been made under this section.

118 Available at http://www.wipo.int/wipolex/en/text.jsp?file_id=195747
119 Available at http://www.wipo.int/wipolex/en/text.jsp?file_id=198080

Privacy and data protection laws of Bali Process member States
Viet Nam

The right to privacy is expressly provided for in the Civil Code, which provides that an individual’s rights to personal secrets shall be respected and protected by law, the collection and publication of information of the private life of an individual must be consented to, and that the confidentiality of correspondence is guaranteed, unless provided for by law.\(^{120}\)

While there is no consolidated privacy or data protection law, privacy protection is provided in various laws, including the Law on Information Technology 2006 (LIT),\(^{121}\) the Law on E-Commerce and the Law on Consumer Protection. This report will focus on the LIT since it has the most applicability to government agencies.

**Law on Information Technology 2006**

The LIT provides for “measures to ensure information technology application and development, and rights and obligations of agencies, organizations and individuals (hereinafter collectively referred to as organizations and individuals) engaged in information technology application and development activities.” Under Article 7, the Ministry of Post and Telematics has “prime responsibility for, and coordinating with concerned ministries and ministerial-level agencies in, performing the state management of information technology.”

**Scope and application**

Under Article 2, the LIT applies to Vietnamese and foreign organizations and individuals engaged in information technology application and development activities in Vietnam. This includes State agencies.

Under Article 4, the LIT applies to digital information, which means information generated by the method of using digital signals.

**Collection and notification**

Under Article 21, organizations and individuals that collect personal information are responsible for informing people of the form, scope, place and purpose of collecting, processing and using their personal information.

**Use and disclosure**

Under Article 21, organizations and individuals that process and use personal information are responsible for use of the collected personal information for proper purposes. Consent is generally required unless provided for by law, including when it is being used for the following purposes:

- signing, modifying or performing contracts on the use of information, products or services in the network environment;
- calculating charges for use of information, products or services in the network environment; or
- performing other obligations provided for by law.

---


Organizations or individuals may not supply personal information to a third party unless otherwise provided for by law or there is consent from the individual concerned.

Cross-border transfers

The LIT is silent on any specific requirements in relation to cross-border transfers of personal information.

Access and correction

Under Article 22, individuals may request organizations or individuals that store their personal information in the network environment to “inspect, correct or cancel such information.” Organizations and individuals are required to immediately take necessary measures to refrain from supplying or using relevant personal information until it is corrected.

Retention

Under Article 21(2)(b), organizations and individuals can store personal information only for a given period of time set by law or as agreed upon by the two parties.

State agencies

Under Article 24, State agencies have additional principles for information technology application that are broadly consistent with some of the common privacy principles. These principles are:

1. The application of information technology to the operation of state agencies must be prioritized and ensure publicity and transparency with a view to raising the effectiveness and efficiency of operation of state agencies and creating conditions for people to well exercise their civil rights and duties.

2. The application of information technology to operation of state agencies must promote the program on renewing the operation of state agencies and the administrative reform program.

3. Supply and exchange of information must ensure its accuracy and suitability to use purposes.

4. Operation processes and procedures must be made public and transparent.

5. Using uniform standards, ensuring technological compatibility in the entire information system of state agencies.


7. Heads of state agencies shall be responsible for information technology application under their management.

Enforcement

Under Article 75, settlement of disputes over information technology occurs first through conciliation, and then in accordance with law, which presumably includes court procedures.

Under Article 77, violations of the LIT, depending on the nature and severity, may result in administrative sanctions, penal liabilities or compensation against the violating individuals or organizations.
The Bali Process