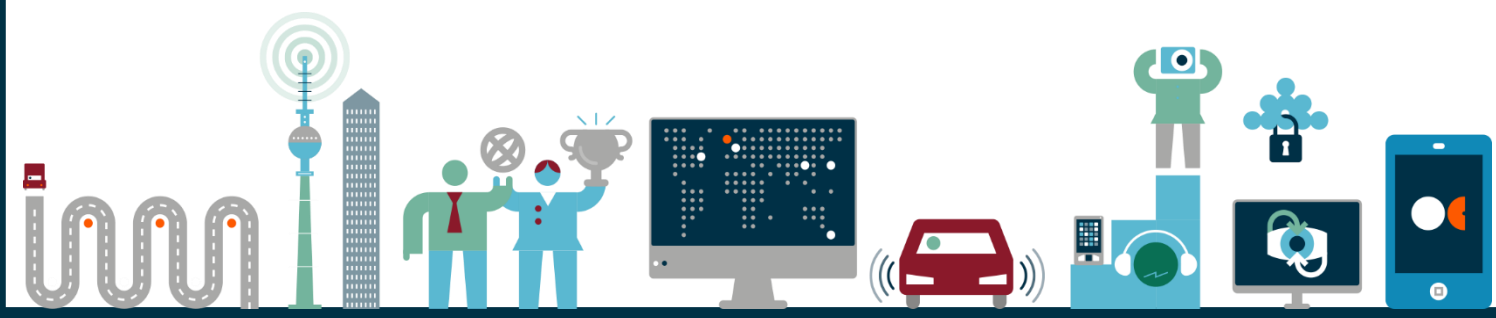
#	Subject	The ADPPA compared with the GDPR
1	**Covered Data vs. Personal Data**	The ADPPA does not apply to the same scope of *personal data* covered by the GDPR. **Covered data** in the ADPPA is defined as information that identifies or is linked or reasonably linkable to individuals (Sec. 2 (8) (A) ADPPA) but excludes (i) de-identified data, (ii) employee data, and (iii) publicly available information (as well as inferences made from such information).
2	**Individuals vs. Data Subject**	**Individual** refers to the person who the **covered data** relates to, so it is comparable to the GDPR-term of *data subjects*. However, the term **individuals** covers only those that reside in the U.S. (Sec. 2 (16) ADPPA). Consequently, individuals residing in the EU shall not enjoy the protection of the ADPPA when their *personal data* will be processed by **covered entities**.
3	**Roles under the ADPPA**	The ADPPA differentiates between the following main roles for a person or an entity that is subject to the ADPPA: **Covered entity** (corresponding to the role of a *controller* under the GDPR), **service provider** (corresponding to the role of a *processor* under the GDPR), and **third parties** (somewhat similar to a *data recipient* under the GDPR that qualifies as *controller*).
3a	**Covered Entities vs. (Joint) Controllers**	The role of a **covered entity** under the ADPPA is comparable to the role of a *controller* under the GDPR. The majority of the privacy obligations established by the ADPPA are directed at the **covered entity**. **Covered entity** is defined as (i) the entity or person that alone or jointly with others determines the purposes and means of collecting, processing, or transferring **covered data** and (ii) that is subject to the Federal Trade Commission Act, the Communications Act of 1934 or is a non-profit organization (Sec. 2 (9) ADPPA). An entity that controls or is controlled by or is under common control with another covered entity is included by the term **covered entity** (Sec. 2 (9) (d) (ii) ADPPA). This seems to suggest that the ADPPA does not distinguish as strictly between the various legal entities belonging to the same group as the GDPR does, but rather takes the group as a whole into account. Federal, State, or other government entities are not covered by the term **covered entity** (Sec. 2 (9) (C) ADPPA).



3b Service Providers vs. Processors

The role of a **service provider** under the ADPPA is comparable to the role of a *processor* under the GDPR.

The ADPPA imposes certain privacy obligations on **service providers** as well as on **covered entities** when contracting with **service providers**. The definition of **service providers** (Sec. 2 (25) ADPPA) largely corresponds to the definition of *processors* as per the GDPR, referring to a person or entity that processes **covered data** on behalf and at the direction of the **covered entity**.

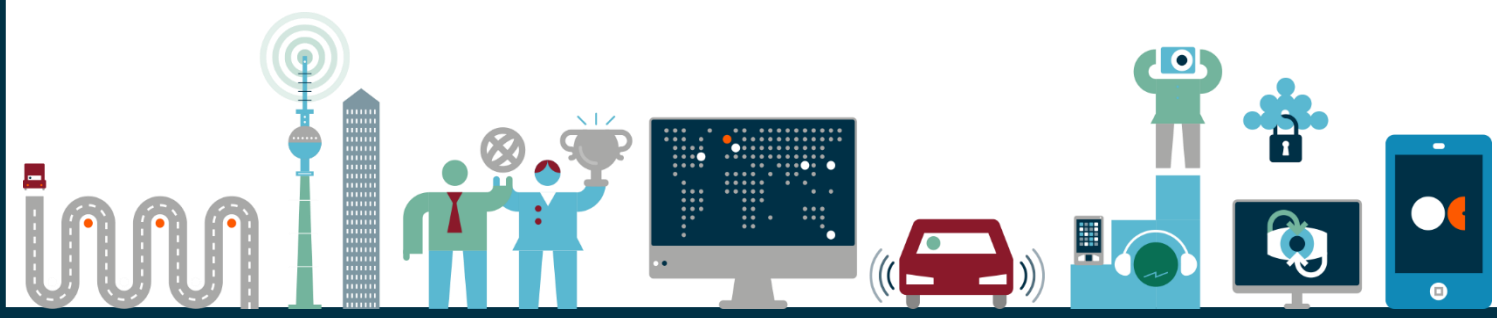
Similar to the relationship between *controller* and *processor* under the GDPR, **covered entities** and **service providers** are required to conclude a contract specifying the details of the processing as well as the respective rights and obligations (Sec. 302 (b) ADPPA). One notable difference, however, is that a **covered entity** is not liable for any data protection violations of its **service provider** if it has complied with the ADPPA when transferring data to said **service provider** (Sec. 302 (c) (2) ADPPA).

3c Third Parties

A **third party** is defined by the ADPPA as any person or entity that processes **third party data** (i.e., **covered data** transferred by a covered entity), without being a **service provider** for such data (Sec. 2 (31) ADPPA). The concept of a **third party** is somewhat comparable to a *controller* under GDPR that receives personal data from another *controller*.

The transfer of **covered data** to such a **third party** by a **covered entity** is subject to certain requirements (see no. 10 below) and specific obligations are attached to the role of such a **third party** when they process **covered data** (Sec. 302 (d) ADPPA).

The term **third party** does not include an entity that processes covered data which it has received from an affiliate (Sec. 2 (31) (B) ADPPA) unless one of the entities involved is a **large data holder**. This exclusion of affiliates from the term **third party** may result in a privilege for data transfers within a group of companies as such data transfers would seem to be excluded from the requirements for transfers to **third parties** (see no. 10 below). This deviates from the concept of the GDPR where data transfers within a group of companies are subject to the same legal requirements as transfers to external parties.



3d	**Large Data Holders**	The ADPPA qualifies **covered entities** and **service providers** as **large data holders** if they have a gross annual revenue of at least USD 250 million and they collect, process or transfer the **covered data** of more than 5 million **individuals**, with the latter threshold reduced to 200.000 individuals for **covered sensitive data** (Sec. 2 (17) ADPPA). **Large data holders** are subject to special obligations, in particular with respect to transparency obligations (Sec. 202 (e) (4) and (f) ADPPA), individual's rights (Sec. 203 (c) ADPPA) and privacy impact assessment obligations (Sec. 301 (d) ADPPA). They also have to carry out a so-called **algorithmic impact assessment** (Sec. 207 (c) ADPPA). Such an assessment is not required under the GDPR but seems to be comparable with the assessments envisioned under the EU's planned Artificial Intelligence Act.
4	**Duty of Loyalty vs. Data Privacy Principles**	Title I of the ADPPA establishes the **duty of loyalty**, including general principles for the processing of **covered data** similar to the key principles provided by Art. 5 GDPR. Those general principles include, inter alia, requirements on data minimization, necessity, and proportionality, the obligation to demonstrate compliance, and the principle of privacy by design.
5	**Permissible Purposes vs. Legal Bases for Processing**	**Covered data** shall not be processed unless it is reasonably necessary and proportionate for (1) a specific product or service requested by the individual, (2) a reasonably anticipated communication with the individual, or (3) a purpose expressly permitted by the ADPPPA (Sec. 101 (a) ADPPA). Sec. 101 (b) ADPPA provides an exhaustive list of such **permissible purposes**. These **permissible purposes** have some similarities to the legal bases provided by Art. 6 (1) (b) to (e) GDPR. They also include aspects that from a GDPR perspective could qualify as a legitimate interest under Art. 6 (1) (f). However, unlike Art. 6 (1) (f) GDPR, the ADPPA does not provide for a generic term of legitimate interest with some degree of flexibility; instead, the ADPPA defines interests of the covered entity that are considered legitimate and that permit a data processing activity in an exhaustive manner. On the other hand, the ADPPA does not require a balancing of the interests as provided by Art. 6 (1) (f) GDPR. Sec. 101 (a) ADPPA does not provide for consent as a ground for processing (instead, consent is required in some circumstances, see no. 6 below). However, processing operations which may require consent under the GDPR, such as first party marketing, are included in the list of **permissible purposes**.

6	**Affirmative Express Consent**	Valid consent under the ADPPA refers to an **affirmative express consent** (Sec. 2 (1) (A) ADPPA) which requires the **individual's** freely given, specific, informed, and unambiguous authorization for an act or practice that is clearly communicated in response to a specific request from a **covered entity**. Said request must be provided in a standalone disclosure and meet comprehensive transparency requirements (Sec. 2 (1) (B) ADPPA). The individual's inaction or continued use of a service or product does not suffice to establish said consent (Sec. 2 (1) (C) ADPPA) even if the covered entity enabled the individual to opt out. These requirements largely correspond to the requirements of a valid consent under GDPR. **Affirmative express consent** is only required for a few data processing operations under the ADPPA, including transfers of **sensitive covered data** to **third parties** (Sec. 102 (a) (3) (A) ADPPA).
7	**Privacy Policy vs. Data Protection Declaration**	**Covered entities** and **service providers** are required to provide a privacy policy (Sec. 202 ADPPA). The required information (see Sec. 202 (b)) largely corresponds to those required under Art. 13/14 GDPR. Any material change of a privacy policy triggers the obligation to notify the affected **individuals** and provide opportunity to withdraw consent to materially different processing. Such privacy policy must also disclose if **covered data** shall be transferred to The People's Republic of China, Russia, Iran, or North Korea.
8	**Sensitive Covered Data vs. Special Categories of Personal Data**	Similar to the GDPR, the ADPPA provides additional protection for sensitive data which are referred to as **sensitive covered data**. **Sensitive covered data** (Sec. 2 (24) ADPPA) covers a wider range of data categories, not only health data, biometric genetic data, and sexual orientation as covered by the *special categories of personal data* under the GDPR, but also government-issued identifiers, financial account numbers, precise geolocation, private communication, log-in credentials, calendar information, address book information, private photos and videos, information on video content or services requested by the **individual** from a broadcasting or streaming provider, information relating to **individuals** under the age of 17. Unlike the concept of *special categories of personal data* under the GDPR, it does currently not include race, ethnic origin, religion, or union membership.

		Processing of **sensitive covered data** is only permitted if strictly necessary for a specific product or service requested by the individual or for certain of the **permitted purposes**, excluding in particular the purpose of first party marketing (Sec. 102 (a) (2) ADPPA). Transferring **sensitive covered data to third parties** is also subject to further restrictions (Sec. 102 (a) (3) ADPPA).
9	**Protection of Minors**	Information about minors under the age of 17 is generally qualified as **sensitive covered data** when the **covered entity** knows the **individual** is under the age of 17 (Sec. 2 (24) (A) (xiii) ADPPA). Targeted advertising is prohibited with respect to such minors and data transfers to **third parties** require consent (Sec. 205 ADPPA).
10	**Data Transfers**	A **transfer** is the disclosure of data by transmission regardless of whether or not the recipient is located in the U.S. **A transfer** of **covered data** is generally permitted if it is reasonably necessary and proportionate for (1) a specific product or service requested by the individual, (2) a reasonably anticipated communication with the individual, or (3) a purpose expressly permitted by the ADPPA (Sec. 101 (a) ADPPA). However, in the case of a transfer of covered data to a third party that relies on Sec. 101 (a) (1) or (2) of the ADPPA, the individuals have a right to opt out of such a transfer (Sec. 204 (b) ADPPA). Additional requirements apply if **sensitive covered data** shall be transferred to **third parties** (Sec. 102 (a) (3) ADPPA).
11	**International Data Transfers**	Unlike the GDPR in Chapter V, the ADPPA does not provide for additional requirements for international data transfers.

12	**Consumer Data Rights vs. Data Subject's Rights**	Title II of the ADPPA (Sec. 201 et seqq. ADPPA) provides for **consumer data rights** similar to the data subject rights in the GDPR. These rights under the ADPPA include the right to be informed on the data processing as well as the rights of access to, correction, deletion and portability of **covered data** and to opt out of targeted advertising. However, in comparison to the *data subject's rights* under GDPR, the **consumer data rights** are subject to certain limitations. For example, back-up and archived data are excluded from the access right, the scope of access is restricted to the data processed within the last 24 months, and, depending on the size of the covered entity, the statutory response time is between 45 to 135 days (Sec. 203 ADPPA). **Covered entities** may rely on certain exceptions to refuse answering a request. Similar to the GDPR, service providers are obliged to take appropriate technical and organizational measures to assist covered entities in fulfilling individual rights requests (Sec. 302 (a) (3) ADPPA).
13	**Impact Assessment Obligations of Large Data Holders vs. Data Protection Impact Assessment**	Unlike the GDPR, there is no general *data protection impact assessment* requirement that applies to all types of covered entities. Instead, only a **covered entity** or **service provider** qualifying as a **large data holder** is required to (1) assess the privacy impact of its data processing in general (Sec. 301 (d) ADPPA), and (2) assess the use of algorithms in connection with the respective data processing, if applicable, and provide this assessment to the FTC (Sec. 207 (c) (1) ADPPA).
14	**Privacy Officers vs. Data Protection Officers**	**Covered entities** and **service providers** must designate qualified employees as **privacy officers** and **data security officers** (Sec. 301 (c) ADPPA). The responsibilities of the designees depend on whether or not the respective entity qualifies as a **large data holder**. Unlike the GDPR, there are no thresholds that trigger the designation requirement as the ADPPA provides for a general designation requirement.

15	**Data Security Practices vs. Technical and Organizational Measures**	**Covered entities** and **service providers** are required to implement reasonable administrative, technical, and physical data security practices and procedures against unauthorized access and acquisition of **covered data** (Sec. 208 ADPPA) taking aspects similar to those set out in Art. 32 GDPR into account. A list of specific data security practices to be implemented as a minimum is provided in Sec. 208 (b) ADPPA). As part of the requirements for privacy by design, covered entities and **service providers** must establish policies, practices and procedures to address privacy risks and implement training and safeguards.
16	**Private Right of Action and Enforcement**	Like the GDPR, the ADPPA provides for enforcement by governmental authorities as well as by individuals. However, there are significant differences, both in the respective enforcement regimes themselves and in the relationship between them. The governmental authorities with the competence to enforce the ADPPA shall be the FTC on a federal level (Sec. 401 ADPPA) and the state attorneys general on the state level (Sec. 402 ADPPA). Neither of them is equipped with privacy specific enforcement instruments. The FTC, for example, can enforce violations of the ADPPA as violations of a rule defining an unfair or deceptive act or practice under the FTC Act. The ADPPA's **private right of action** (Sec. 403 ADPPA) allows individuals to pursue claims similar to Art. 82 GDPR, namely to seek damages/compensation. While Art. 82 GDPR exists independently from enforcement by the authorities, though, the private right of action is limited to cases where the FTC and the respective state attorney general decide not to act after having been notified of the case by the **individual**.
17	**Pre-emption**	The ADPPA shall pre-empt any state privacy laws that govern aspects already covered by the ADPPA with very limited exception. This approach is similar to the GDPR which does – in general – not allow any member state laws to govern privacy law issues unless expressly permitted by an opening clause of the GDPR. However, the pre-emption clause in the ADPPA is highly debated in the U.S., especially by stakeholders from California.