Personal Data Protection Law of Thailand: Accuracy, Access and Correction of Personal Data

Actions based on inaccurate personal data may result in bad business decisions and may cause harm to consumers. Data is the fuel which drives business decision making. This is particularly true in the social media, advertising, healthcare, banking and insurance sectors. The importance of data accuracy is set to skyrocket. 5G networks and the Internet of Things ("**IoT**") will make datasets even larger and their insights even more accurate and powerful.

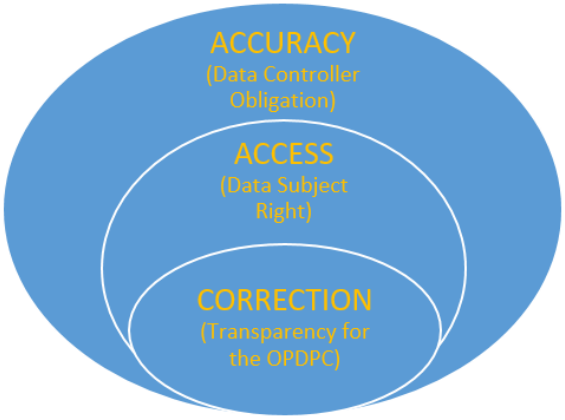
Sections 30, 35 and 36 the Personal Data Protection Act B.E. 2562 ("**PDPA**") mandate the Personal Data Controller ("**Controller**") to safeguard the accuracy of personal data so that data subjects will not be harmed by inaccurate data.

Accuracy
The Controller must ensure that the personal data which it has collected and kept remains accurate and up-to-date and is not misleading.

Access
The PDPA has given data subjects the right to access their own data kept by the Controller by requesting actual access to or by obtaining a copy of their personal data. If any data subject finds his/her personal data incorrect, he is entitled to request that it be corrected.

Correction
The PDPA does not give data subjects a right to correct their own personal data. The PDPA, however, gives them the right to request the Controller to correct their personal data kept by the Controller. If so requested, the Controller must correct the data except in case where the Controller finds the requested changes inappropriate. In such case, the Controller can reject the request but it must state the reasons for rejecting such request in its register. The register must be open to scrutiny by both the OPDPC and the data subject.

Interplay between Accuracy, Access and Correction



The Accuracy, Access and Correction principles

work together as a cohesive multi-layered unit to tackle the issue of dataset inaccuracy. The Accuracy is the first layer. It imposes an obligation on the Controller to ensure that the personal data it has collected is up to date, accurate and not misleading. The Access gives data subjects the right to view their own personal data and thus request for amendments where there are mistakes. This second layer ensures that all stakeholders are a part of the correction process to ensure accuracy. Lastly, the Correction provides transparency in the correction process rather than mandating that personal data must always be amended at the request of a data subject, which may equally lead to inaccurate results. Requiring the Controller to provide reasons why it did not amend the personal data in its register when requested by the data subject makes it possible for the OPDPC to check whether or not the rejection of the request to correct the data is legal.

Risks

Violations of the principles of accuracy, access and correction of personal data can result in fines of up to THB1,000,000 (Section 82 of the PDPA) and compensation for actual damages suffered by the data subject plus punitive damages up to two times of the actual damages (Section 78 of the PDPA). The most important risk, however, is a reputational risk. A failure to adhere to these three principles sends a message to consumers that the Controller business is not concerned with the accuracy of its dataset and does not care about its consumers.

Measures to Mitigate Risks

To mitigate the risks violating Sections 30, 35 and 36 of the PDPA, businesses can:

(1) Review their data collection methods for any inaccuracy which may result in the collection of incorrect personal data.

(2) Conduct an audit of their personal datasets for accuracy and develop/implement.

(3) Methodologies to ensure that personal datasets are maintained and accurate for as long as they are required.

(4) Design and implement a system which personal data subjects can use to easily request and access their personal data.

(5) Provide a detailed and clear set of instructions for data subjects to request for access to their personal data.

(6) Develop a system (physical or online) by which all refusals of personal data amendments are logged in a centralized register with the reasons for each refusal.

(7) Ensure that the above mentioned register can be easily and securely accessed by the OPDPC and data subjects.

(8) Seek legal advice on creating an objective criteria by which all requests to amend are screened.

LawPlus Ltd.
Revised: January 2020

Download PDF

AUTHOR

Kowit Somwaiya
Managing Partner | **Bangkok**
kowit.somwaiya@lawplusltd.com

Jia Xiang Ang
Coordinator | **Bangkok**
jiaxiangang@lawplusltd.com

LawPlus Ltd.
Unit 1401, 14th Floor, Abdulrahim Place 990
Rama IV Road, Bangkok 10500, Thailand
Tel: +662 636 0662
Fax: +662 636 0663

LawPlus Myanmar Ltd.
Unit No. 520, 5th Floor, Hledan Centre
Corner of Pyay Road and Hledan Road, Kamayut Township,
Yangon, Myanmar
Tel: +95 (0)92 6111 7006
and +95 (0)92 6098 9752