ETDA E-Signature Guideline

On 29th May 2020, the Electronic Transactions Development Agency ("**ETDA**") issued its Electronic Signature Guideline under the Electronic Transactions Act B.E. 2544 ("**ETA**") for individuals and legal entities to use for creating electronic signatures for use with different kinds of electronic transactions.

Types of E-Signatures

The Guideline classifies electronic signatures into 3 types as discussed below.

1. General Electronic Signature

A general e-signature can be made in a form of letters, characters, numbers, sounds or any other symbols created in an electronic format and attached to a data message to establish the association of a particular person as the signatory with the data message and indicate that such person has approved the information contained in that data message. For example, a signature line at the end of an e-mail, a scanned image of a handwritten signature attached to a document, an electronic stylus signature, an act of checking a tick box in the data message.

2. Trustworthy Electronic Signature

A trustworthy e-signature is the reliable electronic signature under Section 26 of the ETA. It is an electronic signature using the Public Key Infrastructure (PKI) format that binds the public keys with respective identities of individuals or legal entities.

3. Trustworthy Electronic Signature with Certificate Issued by a Certificate Provider

This type of e-signature also refers to the reliable electronic signature under Section 26 of the ETA. It is an electronic signature using the PKI format plus a certificate issued by a certification service provider under Section 28 of the ETA.

Validity Requirements

Under the Guideline, each e-signature is legally valid under the ETA if it consists of the following elements:

(1) **Signatory Authentication.** It must be used with the electronic data to establish the relationship between its signatory and the electronic data by identifying the signatory. The reliability of the e-signature will link to the reliability of the authentication process.

(2) **Signing Intention.** It must indicate that the signatory intends to be bound by the information contained in the electronic data signed with the e-signature. It must show that the signatory has accepted such electronic data.

(3) **Information Integrity.** The information contained in the electronic data signed with the e-signature must be kept in full without any alteration throughout the retention period with reliable evidence or a third party capable of verifying that no amendment has ever been made to the information contained in the electronic data.

Kowit Somwaiya
Managing Partner
kowit.somwaiya@lawplusltd.com

Oramart Aurore Saardphak
Associate
oramart.saardphak@lawplusltd.com

LawPlus Ltd.
Unit 1401, 14th Fl., Abdulrahim Place, 990 Rama IV Road, Bangkok 10500, Thailand
www.lawplusltd.com