MLR
LEGAL & TAX

**(Non-official Translation)**

**The Republic of the Union of Myanmar**

**The State Administration Council**

**The State Administration Council Law No. (7/2021)**

**The Law Amending the Electronic Transaction Law**

**The 4th Waxing of Tabodwe, 1382 M.E.**

**15th February, 2021**

1. The State Administration Council enacted this Law in accordance with section 419 of the Constitution of the Republic of the Union of Myanmar.
2. This law shall be called the Law Amending the Electronic Transaction Law.
3. Sub-section (a) of Section 2 of the Electronic Transaction Law shall be substituted as follows:

   (a) **Information** means Data, Text, Image, Voice, Video, Code, Software, Application and Databases.

4. After sub-section (k) of section 2 of the Electronic Transaction Law, sub-section (l) sub-section (m), sub-section (n), sub-section (o), sub-section (p), sub-section (q), sub-section (r) and sub-section (s) shall be added as follows:

   (l) **Personal information** means any information which has been verified or verified in relation to a person.

   (m) **Person responsible for maintaining personal information** means the person and its employees assigned by the government department, the

organization authorized to collect, gather, and use personal information under the existing law or in accordance with the provisions of this Law.

(n) **Administration** means the collection, receiving, transferring, distribution, coordination, prohibition, destruction, recording, maintenance, storing, changing, retrieval of stored data, suggestions, utilization or disclosures of personal information.

(o) **Cyber source** means a computer, computer system, computer program or program, network, communication equipment and information.

(q) **Malware** means malicious code that disrupts or endangers a cyber source.

(r) **Cyber Space** means an environment on which electronic information can be sent, communicated, distributed and received reciprocally within a network or by connecting networks by using information, data collection, electronic information, computer programs, software, application with the use of cyber source in information technology-based network system.

(s) **Cyber-attack** means violation of, an attempt, abetment, motivation or acting as a conspirator to violate an attack that targets the executive, finance, economy, rule of law, national security or public safety and property by using a cyber source within a cyber space.

5. Sub-sections (l), (m), (n) of Section 2 of the Electronic Transaction Law shall be renumbered as sub-sections (t), (u) and (v).

6. Sub-section (e) of Section 3 of the Electronic Transaction Law shall be added as Sub-section (f) as follows:

" (f) To be able to protect the personal information of the public in accordance with the law."

7. Chapter 10 of the Electronic Transaction Law shall be supplemented as follows:

## Chapter (10)

### Protection of personal information

27 A. The person responsible for maintaining the personal information shall:

(1) carry out systematically maintaining, protection and managing the personal information based on its type, level of security in accordance with the law.

(2) not allow, disclose, inform, distribute, delivery, reform, destruct, copy and submit as an evidence of the personal information of an individual to any other person or organization, except with the permission of the owner of the personal information or the permission in provision of an existinh law.

(3) not use personal information for the managing matters that are inconsistent with the purpose.

(4) systematically destroy the personal information collected to be used for a limited time beyond the specified time.

27B. Under an existing law, any investigation team that receives information, including personal information or the person who has been delegated or directed under it shall keep the obtained information confidential except as required by law to disclose.

27C. The following matters shall not apply to personal information management matters:

(1) Prevention, search and inquiry, investigation, submission as an evidence in a court by the government department, investigation team or rule of law team assigned by the Central Body for cyber security, cyber-attacks, cyber misuse, cyber-accidents or cybercrime;

(2) Search and inquiry, investigation, information collection, filing and submission as an evidence in a court by government department, investigation team or rule of law team assigned by the Central Body under the jurisdiction on criminal cases;

(3) Inquiry, investigation, data collection and information sharing and coordination carried out under the administrative authority if the cyber security and cybercrime issues concern to the sovereignty of the State, peace and stability, national security;

(4) In administering the matters under sub-section (3), the Central Body or the department or organization assigned by the Central Body defining administrative authority and administering in accordance with those definitions.

8. Chapters (10), (11), (12) and (13) of the Electronic Transaction Law shall be renumbered as Chapters (11), (12), (13) and (14).

9. After section 38 of the Electronic Transaction Law, section 38-A; 38 B, 38-C, 38-D and 38-E must be added as follows:

"38A. If the person responsible for maintaining personal information is found guilty of failing to manage personal information in accordance with the provisions of this law, that person shall be punished with imprisonment for a term of not less than one year and not more than three years or a fine not exceeding 100 lakhs or both.

38B. If any person is convicted of receiving, disclosing, using, destructing, modifying, distributing, sending or misappropriating personal information of a person to another without the permission of the relevant person, that person shall be punished with imprisonment for a term of not less than one year and not more than three years or a fine not exceeding 50 lakhs or both.

38C. Any person who is convicted of creating misinformation and disinformation with the purpose of causing public panic, loss of trust, defamation or dissolution of association on the cyber, shall be punished with imprisonment for a term of not less than one year and not more than three years or a fine not exceeding 50 lakhs or both.

38D. Any person who is convicted of cyber-attacks such as preventing access to cyber source, making it difficult or attempting to hack into a cyber source without permission, using more than permitted, and installing malware on a computer with the intent to harm someone, with an intent to threaten or disturb the sovereignty of the State, security, peace and stability, rule of law or national unity, shall be punished with imprisonment for a term of a minimum of two years and a maximum of five years or a fine not exceeding 300 lakhs or both.

38E. Any person who commits acts of cyber-attacks such as without permission attempting access to and hacking cyber sources which are kept confidential in cooperation between the country and other countries for security reasons and using more than permitted, with the intent of deteriorating the close relationship between the country and other foreign countries or for the interests of other foreign country, shall be punished with imprisonment for a term not exceeding three years and not more than seven years or a fine not exceeding 500 lakhs or both."

……

I sign under section 419 of the Constitution of the Republic of the Union of Myanmar.

MLR
LEGAL & TAX

Min Aung Hlaing

Commender-in-Chief

Chairman

State Administration Council



**MLR COMPANY LIMITED**
**Times City – Office Tower n°2 – 16th Floor – Units 11 & 12**
**Between Hanthawaddy & Kyuntaw Road – Kamayut Township – Yangon – Myanmar**
**+ 95 (0) 9 25 21 783 62**
**contact@mlr.ltd**
**www.mlr.ltd**