**Republic of the Union of Myanmar**

**State Administration Council**

**The Law Amending the Electronic Transactions Law**

**The State Administration Council Law No. 7, 2021**

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

**(15 February 2021)**

1. The State Administration Council hereby enacts this Law under section 419 of the Constitution of the Republic of the Union of Myanmar.

2. This Law shall be called **the Law Amending the Electronic Transactions Law**.

3. Subsection (a) of section 2 of the Electronic Transactions Law shall be substituted as follows:

“(a) **Information** means data, text, image, voice, video, code, software, application and database;”

4. After subsection (k) of section 2 of the Electronic Transactions Law, subsections (l), (m), (n), (o), (p), (q) and (r) shall be inserted as follows:

“(l) **Personal data** means any data related to an individual, by which that individual has been identified or is identifiable;

(m) **Controller of personal data** means a person and his or her staff assigned by the government department or organization having the authority to collect, store, and use personal data under any existing law or the provision of this Law;

(n) **Processing** means the collection, receiving, transfer, dissemination, combination, restriction, destruction, recording, preservation, storage, adaptation, retrieval, advice, use, or disclosure of or on personal data;

(o) **Cyber resource** means computer, computer system, computer programme or programme, network, telecommunications equipment, and data;

(p) **Malware** means a malicious code that is designed to disrupt or cause damage to cyber resource;

(q) **Cyber Space** means the space on which electronic information can be sent, communicated, disseminated and received within a single network or interconnected networks by using information, database, electronic information, computer programme, software or application with the use of cyber resources within information technology-based network system;

(r) **Cyberattack** means commission of, attempt to commit, abetment, incitement or conspiracy to commit any attack by using any cyber resource in cyber space with intent to jeopardize the administration, finance, economy, rule of law, national security of the State, or security, life and property of the public.”

5. Subsections (l), (m), and (n) of section 2 of the Electronic Transactions Law shall be renumbered as subsections (s), (t), and (u).

6. After subsection (e) of section 3 of the Electronic Transactions Law, subsection (f) shall be inserted as follows:

“(f) to protect personal data of the public in accordance with law.”

7. Chapter X of the Electronic Transactions Law shall be inserted as follows:

**Chapter X**

**Protection of Personal data**

27-A. A controller of personal data shall:

(i) preserve, protect and process personal data according to their types and levels of security systematically in accordance with law;

(ii) not allow any other person or any organization to inspect any personal data which is under his or her control, or not disclose, inform of, disseminate or sent it to such person or organization, or not alter, destroy or copy it or submit it as evidence except with the permission under any existing law or permission of owner of such personal data;

(iii) not use personal data for processing which is inconsistent with the objectives;

(iv) systematically destroy personal data collected with the intention of using it within a specific time frame, once that specified time frame has been exceeded.

27-B. Any investigation team that receives any information including personal data under any existing law, or any person who is delegated by or under instruction of that team shall keep the information received confidential except having responsibility to disclose it under any law.

27-C. In the case of processing personal data, the following matters shall not be concerned:

(i) prevention, search and detection, investigation, and submission of evidence in any court conducted by the government department or investigation team or law enforcement agency assigned by the Central Body, relating to cyber security, cyberattacks, cyber abuse, cyber incidents or cybercrimes;

(ii) search and detection, investigation, intelligence gathering, prosecution and submission of evidence in any court conducted, under the administrative authority for criminal cases, by the government department or investigation team or law enforcement agency assigned by the Central Body;

(iii) search and detection, investigation, intelligence gathering and integration of information conducted under the administrative authority for cyber security and cybercrimes relating to the perpetuation of the sovereignty of the State, peace and tranquility and the National Security;

(iv) specification of administrative authority by the Central Body or by the department or organization assigned by the Central Body to perform the functions in subsection (iii), and conducting in accordance with the specified authority.”

8. Chapters X, XI, XII and XIII of the Electronic Transactions Law shall be renumbered as Chapters XI, XII, XIII and XIV.

9. After section 38 of the Electronic Transactions Law, sections 38-A, 38-B, 38-C, 38-D and 38-E shall be inserted as follows:

“38-A. A controller of personal data who is convicted of failing to process personal data in accordance with the provisions of this Law shall be punished with imprisonment for a term which may extend from a minimum of one year to a maximum of three years or with a fine not exceeding ten million kyats or with both.

38-B. Whoever is convicted of receiving, disclosure, use, destruction, alteration, dissemination, sending or abuse of personal data without permission of person concerned shall be punished with imprisonment for a term from a minimum of one year to a maximum of three years or with a fine not exceeding five million kyats or with both.

38-C. Whoever is convicted of contriving fake news or false news, with intent to cause fear, loss of trust to the public, disaffection or split in society or group on cyber space shall be punished with imprisonment for a term from a minimum of one year to a maximum of three years or with a fine not exceeding five million kyats or with both.

38-D. Whoever is convicted of cyberattack by obstructing or causing difficulties in access to hindering or attempting to hack cyber resource or overusing the limited cyber resource without permission with intent to threaten sovereignty, security, peace and tranquility of the State, rule of law or national consolidation, or by installing malware on computer with intent to cause harm to someone shall be punished with imprisonment for a term from a minimum of two years to a maximum of five years or with a fine not exceeding thirty million kyats or with both.

38-E. Whoever is convicted of cyberattack by attempting to hack cyber resource which is kept confidential and implemented multilaterally for security among the State and any other States or overusing the limited cyber resource without permission with intent to damage the close relationship between the State and any other States or for the benefits of any other States shall be punished with imprisonment for a term from a minimum of three years to a maximum of seven years or with a fine not exceeding fifty million kyats or with both.”

I hereby sign under the Constitution of the Republic of the Union of Myanmar.

(Sd.) Min Aung Hlaing

Senior General

Chairman

State Administration Council