

COMPUTER MISUSE AMENDMENT ACT ALERT

Computer Misuse Amendment Act.

On 13th October 2022, the President of Uganda signed the Computer Misuse Amendment Act (2022) into law. In it, several changes were introduced that will affect the cyber laws and their application in the country.

This Act not only affects individuals but also all NGOs, local or International, or any other entity handling computer data.

What is the Computer Misuse Amendment Act (2022)?

This Act deals with all use of information or data through a computer and creates offences for unlawful handling of such data.

A computer means any electronic device through which data is stored or shared and can include laptops, phones, or even a computer server among others.

The Act amended the provisions of the Computer Misuse Act of 2011 as per its objectives as discussed below.

Objectives of the Computer Misuse Amendment Act.

- To enhance the provisions on unauthorized access to information or data.
- To prohibit unlawful sharing of any information relating to a child.
- To prohibit hate speech, the sending or sharing of malicious or unsolicited information.
- To regulate the use of social media.

Offences introduced by the Computer Misuse Amendment Act.

1. Unauthorised Access to Information or Data.

The Act penalizes a person who unlawfully /without authority accesses another's person's data or video or voice records another person or shares any information about another person.

Therefore, individuals or Corporations should desist from accessing programs/ personal information without prior consent otherwise they will be held culpable by the law.

COMPUTER MISUSE AMENDMENT ACT ALERT

2. Unlawful sharing of any Information relating to a Child.

The Amendment penalizes sharing of any information that relates to a child through a computer without prior consent of the child's parent/guardian or other person having authority to make decisions on behalf of the child.

The only exception is where the person who shares such information does so with the authority of the law or does so in the best interests of the child.

Therefore, when dealing with personal information relating to children, one ought to first seek consent from their parents or guardians before dealing with such information.

3. Hate speech.

The Amendment penalizes the sharing of any information through a computer, which is likely to;

- (a) Ridicule, degrade or demean another person, group of persons, a tribe, an ethnicity, a religion or gender;
- (b) Create divisions among persons, a tribe an ethnicity, a religion or gender or promote hostility against a person, a group of persons, a tribe or ethnicity, a religion or gender.

Important to note here is that the Amendment Act does not expressly define what amounts to hate speech and its definition is thus subjective as it can vary from one person to another.

Therefore, a person or Organization ought to be very cautious through their communication over the computer or internet so as to avoid being held culpable under the Act.

4. Unsolicited Information.

The sharing of unsolicited information through a computer is an offence. Unsolicited information is defined as information transmitted to a person using the internet without the person's consent or which has not been requested for.

The only exceptions to this are; (a) if such information is in the public interest or (b) it's commercial information, such as commercial adverts.

COMPUTER MISUSE AMENDMENT ACT ALERT

Unfortunately, unsolicited information can, however, be beneficial to the recipient yet the Amendment makes it an offence to share or send such information. Such information includes personal information, information related to education, a person's security, health and wellbeing. All such information can be beneficial to the recipient but may not necessarily fall under public interest.

An individual or Organization should therefore be cautious to only share information requested for or which is of a commercial nature.

5. Malicious Information.

The sending or sharing of malicious information that relates to another person through a computer is an offence under the Amendment Act.

The Amendment unfortunately does not define what amounts to 'malicious information', as this can be subjective as interpreted by different persons.

However, as a reasonable person, if you think of information about another person as being malicious, you ought to exercise caution and not send or share such information over the computer so as not to fall culpable under the law.

6. Misuse of Social Media.

The use of social media to publish, distribute, or share information prohibited under the laws of Uganda under a disguised or false identity is an offence.

Where the information is published, distributed or shared on the social media account of an organisation, the person who manages the social media account of the organisation is personally liable for the commission of the offence.

This is relevant to Organizations, as it places an obligation upon Management to put measures in place to guard against the unauthorized sharing of information on the Organization Social media platforms.

This offence was put in place to regulate the misuse of social media to ridicule or degrade other persons via social media platforms and the like as this vice had become rampant in Uganda.

COMPUTER MISUSE AMENDMENT ACT ALERT

However, the Amendment does not define what ‘prohibited information’ is under the laws of Uganda. People or Organizations should therefore be cautious in handling social media platforms, especially official accounts of Establishments, to ensure that only information relating to the objectives of the Organization is shared.

Notably, the Amendment has done away with the limitation of the accused person being in Uganda at the material time or the computer, program or data being in Uganda at the material time. This has thereby extended the jurisdiction in regard to the location of the accused person or the computer, program or data outside Uganda.

Relevance to Organizations.

Organizations handle data relating to individuals either for employees or even contractors. The use of such information is to be done lawfully and in compliance with provisions that deal with the protection of personal data.

- In collecting the information of its employees, an organization should do so lawfully with the individual’s consent. This can be done with documents such as a ‘consent form’ that an individual signs allowing the Organization to collect their personal data.
- Collection of personal information should either be solicited from the individuals with their consent or from lawful third parties authorized to handle such information through formal processes.
- Information relating to children should be collected with the consent of their parents or guardians and relevant measures put in place for the protection of such information. Any such collection should always be through formal processes.
- Organizations should only publish information relating to their objectives and desist from commenting or sharing information on matters of a tribal, gender, religious or political nature.
- Information should also only be published on official accounts of the Organization, with the Management of the Organization establishing procedures and guidelines on how such information is to be directed to the public. This includes; Social media handles such as; WhatsApp, Twitter and Facebook among others.

Conclusion

As an organization, serious caution should be taken as to the handling and sharing of data be it in the workplace, or even on social media platforms. Policies should be put in place for

COMPUTER MISUSE AMENDMENT ACT ALERT

the handling of data, which should follow a review by the concerned Management before it can be shared either internally or even with the public. Vet any persons handling organisation social media platforms and ensure employees sign an ethics policy on how to handle organisation communication internally and with third parties.

Any violation as regards to the use of data creates an offence with penalties such as imprisonment of up to a term of Seven (7) years or more or a penalty of Fifteen Million Uganda Shillings (UGX 15,000,000).

Alternatively, have your legal advisors review the organisation documents you use for operations, to ensure they comply with the Computer Misuse Amendment Act.

Disclaimer:

The contents of this alert are to guide you in complying with the recent amendment to the Computer Misuse Act. Should you require independent advice, please contact us at the address below.

LIBRA Advocates & Consultants

2nd Floor – AHA Tower, opp. Min. of Health HQ,
Plot 7 Lourdel Road, Nakasero
P. O. Box 28392, Kampala
Tel: 0392081345 / 0200903575
E-mail: info@libraconsultantsug.com
W: www.libraconsultantsug.com