Promoting Professionalism in Accountancy

INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS OF UGANDA

DATA PROTECTION AND PRIVACY GUIDELINES

NOVEMBER 2019

Plot 42 Bukoto Street, Kololo, P.O. Box 12464, Kampala, UGANDA
Tel: 041-4540125, 0393-262-333, 0393-265-590
standards@icpau.co.ug
www.icpau.co.ug

DISCLAIMER

This Paper contains general guidance to ICPAU members that is indicative of the regulatory requirements and good practice in data protection and privacy.

The Paper is not intended to be comprehensive or to deal with all situations that might be encountered. This Paper is supplementary to and is not a substitute for reading the Data Protection and Privacy Act 2019 and other relevant laws and regulations, which should be regarded as the primary source of guidance.

The information provided in this Paper does not, and is not intended to, constitute legal advice. If in doubt, ICPAU members are advised to seek appropriate legal advice.

Whereas every care has been taken in the preparation of this paper, the ICPAU disclaims any responsibility or liability that may occur, directly or indirectly, as a consequence of the use and application of the Paper.

TABLE OF CONTENTS

ABOUT ICPAU

The Institute of Certified Public Accountants of Uganda (ICPAU) was established in 1992 by the Accountants Act, Cap 266. This has now been repealed and replaced by the Accountants Act, 2013.

The functions of the Institute, as prescribed by the Act, are to regulate and maintain the Standard of Accountancy in Uganda; and to prescribe and regulate the conduct of accountants and practising accountants in Uganda. Under its legal mandate, the Institute prescribes professional standards to be applied in the preparation and auditing of financial reports in Uganda.

Vision

To be a world class professional accountancy institute.

Mission

To develop and promote the accountancy profession in Uganda and beyond.

Core Values

1) Professional Excellence
2) Accountability
3) Integrity
4) Innovation

International Affiliations

The Institute is a member of the International Federation of Accountants (IFAC) and the Pan African Federation of Accountants (PAFA).

INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS OF UGANDA

DATA PROTECTION AND PRIVACY GUIDELINES

1.0 BACKGROUND

The Data Protection and Privacy Act 2019 (the Act) aims to protect the privacy of individual and their personal data.

Data privacy is about authorized access to personal data i.e. who has the data and who defines access to it. Data protection is the legal mechanism of securing data against unauthorized access.

The Act has a number of objectives, namely:
(a) To protect the privacy of the individual and personal data;
(b) To regulate the collection and processing of personal information;
(c) To provide for the rights of the persons whose data is collected;
(d) To provide obligations of data collectors and data processors; and
(e) To regulate the use or disclosure of personal information and for related matters.

The Act provides the much-needed protection and safeguards for handling personal identifiable information which is particularly important in the digital age.

2.0 PERSONAL DATA AND PRIVACY

Under Section 2 of the Act, personal data refers to any information about a person from which the person can be identified, that is recorded in any form and includes data relating to: the nationality, age or marital status of the person; the educational level, or occupation of the person; an identification number, symbol or other particulars assigned to a person; identity data; or other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual.

The Act prohibits the collection and processing (subject to exceptions) of "special personal data", namely; personal data relating to religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records.

3.0 PRINCIPLES OF DATA PROTECTION

The Act lays down the principles that every data collector, controller or other person collecting or processing data must comply with, including: being accountable to the data subject for data collected, processed or used; ensuring that the collection and processing of the data is fair and lawful; ensuring the collection, processing, use and holding of only necessary and not excessive personal data; retaining personal data for the authorised period for which it is required; ensuring quality of the information collected, processed, used or held; ensuring transparency and participation of the

data subject in the collection, processing, use and holding of the personal data; and, observing security safeguards in respect of the data.

4.0 PRIVACY RIGHTS

The Act aims at bringing improving Uganda's legal framework regarding data protection and privacy in line with international standards and best practices.

The obligations imposed by the Act now require of the data processor, data collector and data controller to dutifully respect and protect the privacy of the persons whose data they collect, store and process.

The following rights are now recognised in the Act.

4.1 Right to be informed

The Act gives data subjects the right to be informed about the nature and category of the information being collected, the purpose for which the data is required, the existence of the right of access to and the right of rectification of the data collected, the period for which the data will be retained to achieve its purpose, among others.

4.2 Right of Consent

The Act prohibits collecting and processing of personal data without prior consent of the data subject and this consent must be freely given, specific, informed, and clearly indicated by a statement or positive action without undue influence.

4.3 Right of Access

The Act gives data subjects the right to request for information on their personal data held or processed by a data controller. Such requests must be responded to without undue delay, in any case within one month of receipt of the request.

4.4 Right of Specification

Under the Act gives data controllers will only have the right to collect data for the specific and explicit purpose that they define and notify the data subject about. The Act adopts the 'minimality' principle, which prohibits a data controller from putting the data to another purpose without the prior informed consent of the data subject.

4.5 Right to be forgotten

The Act introduces the right to be forgotten. Data subjects have the right to request for the correction, removal or erasure of personal data in cases where the data is no longer necessary, inaccurate or misleading. The Act also requires that the data controller will destroy or delete data that the data subject no longer has the right to retain.

5.0 PERSONAL DATA PROTECTION OFFICE

The Act establishes a Personal Data Protection Office (PDPO) under the National Information Technology Authority (NITA) – the Authority, which shall report directly to the Board. The Act further provides that PDPO "shall not be under the direction or control of any person or Authority in performing its functions under this Act".

Amongst its several responsibilities, the PDPO is responsible for:
(a) overseeing the implementation and enforcement of the Act,
(b) creating and keeping a register of all data processing activities and,
(c) receiving and investigating complaints relating to infringement of the rights of the data subject under the Act.

Sanction powers are within the Authority's remit, which seems to have, under the Act, overlapping responsibilities with PDPO, such as keeping and maintaining the register and conducting investigations further to a complaint.

6.0 DATA PROTECTION OFFICER

The Act provides that all institutions must appoint a *data protection officer* who will be responsible for ensuring compliance with the Act. "Institution" is not defined under the Act, but the term could refer to any legal entity, including public bodies and private organisations, such as accounting firms.

7.0 DATA COLLECTION, PROCESSING AND RETENTION

7.1 Processing of personal data

Section 7 of the Act provides the legal basis for processing of personal data. A person shall not collect or process personal data without the prior consent of the data subject. The exceptions to this consent requirement are;
a) permission or obligation by law to process personal data;
b) necessity for public bodies to perform their public duties, national security and for justice and law enforcement;
c) the performance of a contract or entering into a contract to which the data subject is party;
d) for medical purposes; or
e) for compliance with a legal obligation to which the data controller is subject.

The Act, however, under Section 17 allows further processing of data lawfully collected, when such processing is for historical, statistical or research purposes and the person responsible for the processing ensures that;
i) the further processing is carried out solely for the purpose for which the data was collected, and
ii) that the data is not published in a form likely to reveal the identity of the data subject.

7.2 Rights of Data Subjects

Under the Act, data subjects can exercise several rights, including the rights to: access personal information, withdraw consent, prevent processing of personal data, including for direct marketing, object to data processing for automated decision-making, to have the data rectified, blocked or erased, subject to the filing of a complaint before the Data Protection Authority.

7.3 Retention of Records of Personal Data

The Act requires data controllers to retain the data for a period required or prescribed by law; or retain the data for a period which shall afford the data subject an opportunity to request access to the data.
The data must only be held for the purpose for which it was collected and only for as long as is necessary.

7.4 Processing Personal Data outside Uganda

The Act provides that where a data collector or processor based in Uganda processes or stores personal data outside the country, they must ensure that the other country has adequate measures in place for the protection of this data; and that the data subject has consented.

7.5 Security of Data

Under the Act, the data controller, collector or processor is responsible for ensuring the integrity of personal data in their possession or control by adopting appropriate, reasonable, technical and organisational measures to prevent loss, damage or unauthorised destruction, access to or processing of the personal data. The Act further requires them to notify the Authority of any data security breaches and remedial action taken.

8.0 OFFENSES AND SANCTIONS

The Act makes it an offence to unlawfully obtain or disclose personal data. It is also unlawful to destroy, delete, conceal or alter personal data. The sale of personal data is also prohibited under the Act.

Where the offence is committed by a corporation a maximum penalty of 2% of the corporation's annual gross turnover may be imposed.

Offence as against individuals may attract fines of up to UGX 4,900,000 (245 currency points) and/or imprisonment of up to 10 years.

9.0 THE ROLE OF INTERNAL AUDITORS

Internal auditors help organizations achieve corporate objectives by keeping a pulse on the consistency of internal business practices. Internal Auditors have a holistic

view of the organization and can therefore a role in evaluating the organization's compliance with the Act.

9.1 Data Privacy Policies and Procedures

The goal of the internal auditor should be to ensure organizational policies and procedures in line with requirements the Act are in place and are followed. The internal auditor should alert management of any gaps in policy compliance.

When reviewing policies and procedures, it is important to think about whether written policies are meeting the needs of clients and adding value to the organization. Policies and procedures should focus on continuous improvement as it relates to how work is performed. There should be a strong internal audit team environment that supports compliance with policies and procedures. A dysfunctional team can impact procedural compliance.

Policies and procedures should be reviewed on an annual basis to ensure policies reflect the changing business environment. Organisations are only as successful as their ability to create products and services that meet the needs of their clients and to deliver these accurately, seamlessly and without error.

Policies and procedures are how organizations maintain efficient and effective practices that support quality products and services. Internal audits are one tool that organizations use to ensure that their products and services are delivered the right way, the first time and every time.

Compliance requires that all policies, training and procedures are reviewed and updated on a regular basis. All this is within the ambit of the internal audit function to advice on.

9.2 Test of Design

During a "test of design," internal auditors review whether the data privacy policies and procedures are available and whether they meet the requirements of the Act. The outcome serves as a first indication as to which policies and procedures need to be developed or amended. Once the relevant documentation is in place, a test of effectiveness can be developed where the internal auditor will test whether the departments, functions and/or processes effectively implemented the controls.

The internal auditor should clearly document evidence received, all tests performed, and the test results (including inquiry dates, who was interviewed, and evidence inspection tests). In cases where the organization considers an area as non-applicable for testing, the reasoning should also be recorded.

9.3 Internal Auditor and the Data Protection Officer

As a strategic partner of the data protection officer, internal auditors can help to guide the organisation strategy, raise awareness, assess the potential risks, identify gaps, and test the remediated procedures.

On the one hand, the internal auditor performs independent assessments and reports on the effectiveness of implemented measures through the testing of controls as defined in the internal audit plan: Based on its capacity of overseeing policies and procedures and monitoring risk-management activities, the internal auditor can give the data protection officer an assurance of the baseline of compliance after the initial audit. Recurrent audits can also showcase the evolving maturity of the data privacy program. On the other hand, the identification of potential weaknesses provides information to the data protection officer in order to orchestrate the next steps to achieve compliance with the Act.

9.4 Internal Audit Plan

The audit plan enables the identified stakeholders to reflect on the use of personal data within the organization. Auditing and being audited is a catalyser of the general level of data protection awareness among all the staff. Also, the data protection awareness will be tested through a review of the effectiveness of privacy training and awareness campaigns. Internal auditors will have an overview of how aware staff are of data privacy risks throughout the organisation and can recommend appropriate improvements.

It is essential that the internal auditor starts off with a full risk assessment of personal data breach. This assessment provides the main guidance on which departments, functions and/or processes should be audited, which one gets priority, and how often each should be audited. The outcome of the risk assessment will depend on the likelihood of occurrence, the impact, and the mitigating controls.

9.5 Audit Approach

In order to test the effectiveness of implemented policies and processes, the internal auditor should take into account the dependencies and interfaces between departments, IT systems, and personal data sets. In case processes, procedures, systems, and records are specific to one team or department within the organization, an audit can focus on one department. In such cases, the internal auditor should audit the policies, processes and supporting IT systems for the entire data life cycle used by the team or department.

In cases where processes and systems are managed centrally or when they are not specific or unique to a particular department, then these processes and systems should be audited across departments. The underlying process to comply with the individuals' *right to be forgotten* is an example where the internal auditor has to take a procedural approach.

9.6 Reporting and Stakeholder Communication

Frequent status reporting, including the evidence collected by the internal auditor, should be accessible to the relevant internal stakeholders who are engaged in data privacy compliance. During the meetings with these stakeholders, the progress with regards to the internal audits should be discussed. Stakeholders can confirm

findings, escalate difficulties, and identify processes and systems that fell short. These meetings will therefore enable the stakeholders to support, update or correct the scope and approach of the internal audit.

10.0 IMPLICATIONS FOR PRACTISING ACCOUNTANTS

Accountants and accounting firms typically process two different types of personal data: client data and firm data.

• 'Client data' is personal data received from clients in relation to professional engagements and practice.

• 'Firm data' is personal data held by a firm in relation to its own management, employees and affairs generally, including marketing databases.

10.1 Type of Personal Data Available to Accounting Firms

Below are some of the services accountants and auditors offer to clients and the type of personal data they interact with;

(a) Audits

During an audit, personal data relating to shareholders, suppliers, customers, employees and others may be processed by the auditor when forming an opinion on the financial statements. Processing of personal data within an audit is of a verification nature and for the most part, the personal data is not collected from the data subject.

(b) Other attestation services

Where members provide other independent attestation services, for example client money audits, it is likely that circumstances similar to those in an audit will apply. ; notably, there will be no intended impact on the data subjects whose personal data may be processed as part of the engagement and that contacting data subjects directly will involve a substantial effort.

(c) Corporate finance services

Where members provide corporate finance related services to publicly listed companies, such as when providing long form, short form or working capital reports in relation to a new listing or rights issue or advice in relation to mergers and acquisitions, it is possible that they may process personal data relating to shareholders, suppliers, customers, employees or other data subjects of the issuer or, where relevant, the acquisition target.

Such processing is subject to confidentiality obligations so as not to affect the price of any financial instrument, the orderly functioning of financial markets or efficient allocation of capital in the economy.

(d) Due diligence services

Members also frequently undertake due diligence reviews on behalf of clients during which they may process personal data relating to shareholders, suppliers, customers, employees or other data subjects of the intended acquisition target.

(e) Forensic and other investigations

Where members are engaged to provide investigative services, for example in response to a regulatory or legal enquiry, they may process a variety of personal data belonging to various types of data subjects, often in large quantities. For many investigatory services, the purpose and means of processing will be determined by the client (or their legal adviser) and the member will be acting as data processor only and not responsible for transparency. However, there may also be circumstances where the member has a degree of independence in determining the purpose and means of processing and would be a controller in their own right and responsible for transparency.

(f) Consulting services

Certain consulting services may involve the processing of personal data, particularly those relating to organisational and human capital management.

In nearly all circumstances, the content of working papers and reports relating to such services are confidential. The law will apply to any individual or organisations dealing with them.

10.2 Manual Records

The law does not only apply to digital processing. It includes the manual/paper records if they are part of a 'relevant filing system'. This means papers stored systematically, for example, in a filing cabinet are included but ad hoc paper files are not.

This means that practising accountants should ensure that they apply the same levels of diligence to paper records as they do digital records and that any decisions made regarding the lawful basis for processing, adhering to data protection principles and upholding data subjects' rights include paper records.

10.3 Rights of Data Subjects

The Act does not create a conflict with the ICPAU's code of Ethics and the concept of client confidentiality. The core requirements for professional confidentiality and integrity will apply in all cases.

The law provides for the rights of data subjects and so the firm needs to be aware of these and set up policies and procedures to deal with them. These include the rights to: access to personal information; withdraw consent; prevent processing of personal data; object to data processing for automated decision-making; have the data rectified, blocked or erased, subject to the filing of a complaint before the Authority.

All these rights require processes to be in place to ensure that they can be met as they may be enforceable in certain circumstances. It is advisable to put in place policies to deal with such requests now rather than waiting until you receive the requests.

Clients and employees, as data subjects, for example can make a claim against a data collector, processor or controller if they can prove they have suffered damage or distress as a result of a breach through application to a Court of competent jurisdiction. This means that the entity's breach response plan should include an assessment of just who could be impacted (and how) by the breach and how this can be remedied.

10.4 Getting Ready for Compliance

Below are a few key steps that practising accountants and accounting firms should be taking to begin the process of getting ready:

(a) *Appoint someone senior to oversee the process*. The Act requires that all institutions appoint a data protection officer who will be responsible for ensuring compliance with the Act. It is therefore essential that a senior member of staff (director, partner, senior manager) takes responsibility for overseeing the process, allocating funds and resources as necessary. The role established by the law is a person within the institution who should be able to advise the institution on its data protection obligations; monitor compliance with the Act; and be the point of contact for related matters.

(b) *Review existing security and amend or update as necessary*. The review can be tailored in line with the complexity of the organisation and IT set-up. Some relatively straightforward security measures worth considering include: the use of encryption technologies for securing data and controls such as restricted access to personal data and the use of a web accessible portal when sharing documents with clients.

(c) It is recommended that members and member firms *review all the data they hold and on what grounds the data is held* (by category). Following on from this review decisions must be made whether they need to hold it and polices drafted accordingly based on what lawful bases for processing are applicable to the personal data held, rights of data subjects that may be applicable and what contracts need review and rewriting.

(d) *Review contracts with clients, suppliers (anyone who processes your data) and employees* to ensure compliance with the provisions of the Act. As the law imposes new obligations on data controllers and data processors, the entity will need to make sure they understand their responsibilities with regard to both client data and firm data. At the very least contracts will need to be updated to reflect the requirements of the law.

(e) *Develop written data protection policies and procedures*. The policies and procedures need only cover those areas which apply to the entity's use of personal data. Policies and procedures should include, but not be limited to, the following: Who is responsible for what and reporting lines, How to recognise and what to do if there is a breach, How to get consent and when you need consent; How to meet requests from data subjects regarding their rights 'to be forgotten,' rectification; Document retention policies; review policies, etc.

(f) *Training of staff* and especially staff who deal with personal data. This should cover things such as good password practices, not opening emails from unknown senders, how to spot suspicious emails, how to recognise a breach has occurred, knowing when to report, and to whom, how to ensure the physical security of computers, laptops and manual/paper records, as well as awareness of the policies and procedures which apply to the entity's use of personal data.

11.0 CHALLENGES IN IMPLEMENTING THE ACT

- Under the Act, prior consent will be required to allow processing of personal data in order to carry out tasks related to business activities when processing is not necessarily justified by a legal obligation or carried out to execute the terms of a contract with an individual.
- The Act does not specify whether "statistical or research purposes" includes marketing, big data and profiling for business purposes or whether this exception is confined to a more orthodox concept such as research and statistics in the public interest by government bodies, research institutes, etc.
- The term "Institution" as used in the Act is not defined.
- The Act does not cover all the questions arising from the emergence of new technologies such as artificial intelligence and block-chain.
- The law does not compel data controllers to have appropriate technical and organisational procedures, which include suitable privacy policies and keeping sufficient records of their processing activities.
- The law will not be fully operational until the regulations are issued.

12.0 CONCLUSION

Certified Public Accountants (CPAs) have the unique position to fulfil and creating awareness about the need for data privacy compliance. In case an organization has not yet embarked on efforts to implement the requirements of the Act, CPAs have the responsibility to highlight that noncompliance can heavily impact the assets of the organization and can result in tremendous penalties and potential reputational damage.

Consequently, the auditor's findings are an effective management tool to advocate the adoption of a proactive and best practice approach toward data privacy compliance.

The organisation's data protection officer should be able to rely on the CPA's expertise and assurance audits to ensure that board and senior management are kept aware of the progress of implementation of the Act.