Cybersecurity, Data Protection and Privacy Webinar

17 March 2022

Agenda

Time	Activity	Presenter
10:05 – 10.10	Welcome Remarks	Trevor Lukanga, Senior Manager, PwC
10:10 – 10:30	Overview of EU's General Data Protection Regulation (GDPR) and Uganda's data protection and privacy regulatory regime	Dorothy Uzamukunda, Manager, PwC Hilda Kamugisha, Manager, PwC
10:30 – 10:45	Compliance obligations and other regulatory requirements for data collectors, controllers and processors	Stella Nakazibwe, Senior Associate, PwC
10:45 – 11:00	Information security management in light of data protection and privacy laws	Peter Ojekunle, Senior Manager, PwC
11:00 – 11:15	A regulator's perspective on personal data protection and privacy	Angella Tugume, Manager, Data Protection Affairs, NITA-U
11:15 – 11:25	Q&A	Dorothy Uzamukunda
11:25 – 11:30	Closing Remarks	Dorothy Uzamukunda

PwC Presenters for the day

Dorothy Uzamukunda
Manager
Tax & Legal Services

Trevor L Bwanika
Senior Manager
Tax

Hilda Kamugisha
Manager
Tax & Legal Services

Peter Ojekunle
Senior Manager
Digital Trust and
Cyber Security

Stella Nakazibwe
Senior Associate
Tax & Legal Services

Overview of EU's GDPR

Presentation by **Dorothy Uzamukunda**
Manager, Tax & Legal Services
PwC Uganda

Introduction to Data Privacy

EU's General Data Protection Regulation (GDPR)

- Data privacy and protection is a human right and is enshrined in many countries' constitutions and international conventions.
- Emphasis is on the right to respect private and family life, the home and correspondences.
- **The General Data Protection Regulation (GDPR)** was drafted and passed by EU in 2018.
- It imposes obligations on organizations anywhere in the world, so long as they target or collect data related to EU citizens and residents.
- Personal data - information that allows a living person to be directly, or indirectly, identified from data that's available. E.g. person's name, location data, or a clear online username, or it can be something that may be less instantly apparent: IP addresses and cookie identifiers can be considered as personal data.
- Penalties of up to 4% of global turnover.

Data protection / privacy principles of the GDPR

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

GDPR penalties issued so far: why compliance is key

Tim Telecom Italia – 2020 (€27.8m/£24m)

- Complaints **about unwanted promotional calls**.
- Customers were getting nuisance calls without having given their consent - registered their telephone numbers on Italy's "do not call" list or explicitly told callers they were revoking consent for such calls. The violations were several and serious, the regulator found, issuing the large fine and 20 "corrective measures" for the firm.

Google – 2019 €50m/£43.2m

- French regulator ruled that the company **had failed to make its consumer data processing statements easily accessible to its users.**
- Also found guilty of **not seeking the consent of its users** to harness their data for targeted advertising campaigns. Google appealed. France's higher court upheld fine.

H&M - 2020 €35.3m/£32.1m

- Fined by German regulators. Company was **secretly monitoring hundreds of its employees**. If workers took holiday or sick leave, they were required to attend a meeting with senior staff at the retail giant on their return. These meetings were recorded, and made accessible to H&M managers without the knowledge of staff. The data collected from the interviews was used to make a "detailed profile" of workers, which then influenced decisions concerning their employment.

*****British Airways – 2020 ((£20m)**

- Through the **data breach, hackers were able to harvest the personal data of about 400,000 people**
- The leaked data included login and travel booking details, names, addresses and credit card information.
- Hack was the result of British Airways' negligence.
- BA's defence: it let customers know as soon as it became aware of the problem, had fully co-operated with investigation, and that it had "made considerable improvements to the security of its systems since the attack.

Marriott International Hotels – 2020 (£18.4m)

- British hotel fined for hack dating back to 2014 but was not uncovered until 4 years later. **Hack exposed the personal details of about 300 million customers** including credit card information, passport numbers and dates of birth. Seven million of those guest records related to people in the UK.
- Similar to the British Airways fine, the ICO initially said it planned to issue a much higher fine of £99m - but lowered the amount later.

Amazon $886.6m (£636m)

- Compliance penalty.
- Luxembourg's National Commission for Data Protection, which claimed the tech giant's processing of personal data did not comply with EU law.
- **Using personal data for the purposes of advertisement**. It appears that rather than actively seeking consent from its users to collect data Amazon instead relies upon the "legitimate interests" legal basis for collecting data.

***Initially, the Information Commissioner's Office (ICO) planned to fine BA £183m - which would have been the largest fine issued under GDPR.

Conclusion

- Data protection is not a regional matter but a global concern.
- The above principles are integrated within most nation's legal and regulatory frameworks, Uganda inclusive.
- Negative impact: fines and reputational damage.
- Organisations therefore need to adopt best practice in order to comply and protect the data they are entrusted with.

Overview of Uganda's data protection and privacy regulatory regime

Presentation by **Hilda Kamugisha**
Manager, Tax & Legal Services
PwC Uganda

pwc

Introduction

The growth of social and economic activities has highlighted the importance of privacy and data protection.

The collection, use and sharing of personal information with third parties has been a concern.

137 out of 194 countries have put in place legislation to secure the protection of data and privacy.

Africa and Asia show different levels of adoption with 61% and 57% of countries having adopted such legislations. The share in the least developed countries is only 48%.

Source: UN Conference on Trade and Development

Uganda is a signatory to several international and regional conventions with privacy provisions

1948: Protection from arbitrary interference with one's privacy, family, home or correspondence.

1995: Protection from arbitrary or unlawful interference with his privacy, family, home or correspondence.

1986: Implied under the right to respect for life and integrity of the person, the right to dignity, and the right to liberty and security of the person.

1990: Protection from arbitrary or unlawful interference with children's privacy, family, home or correspondence.

1994: Children's right to privacy is protected, except for reasonable supervision by parents or legal guardians over the conduct of their children.

Regulatory Framework (1/2)

1995

Constitution
Article 27 protects the right to privacy. It bars any unlawful search, entry or interference with the privacy of any person's home, correspondence, communication or other property.

2002

Anti-Terrorism Act
Provides for the discretionary power of state officials to conduct surveillance without the need to obtain judicial authorisation.

2005

Access to Information Act
Provides that every citizen has a right of access to information and records in the possession of the State or any public body, except where the release of the information is likely to prejudice the security or sovereignty of the State or interfere with the right to the privacy of any other person.

2010

Regulation of Interception of Communications Act
Regulates the surveillance of communications by security services. Telecommunications service providers must enable interception of their services; and store call-related information as directed by the Minister of Information and Communications Technology.

2011

Computer Misuse Act
Provides for the safety and security of electronic transactions and information systems from unlawful access, abuse or misuse and for securing the conduct of electronic transactions in a trustworthy electronic environment.

Regulatory Framework (2/2)

2015 Registration of Persons Act

Provides for the registration of persons and establishes the NIRA which is mandated to maintain a national identification register for all Ugandans.

2019 – Data Protection and Privacy Act

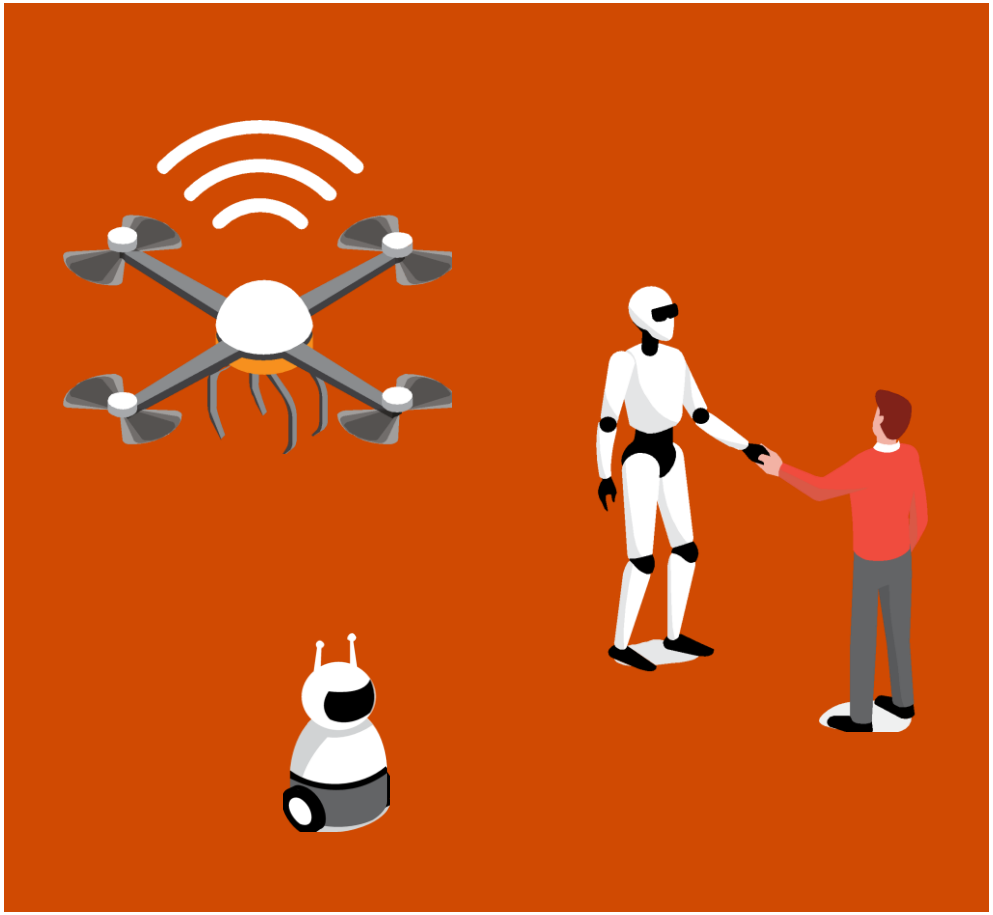
- Regulates personal data collection, processing, use and disclosure.
- Applies to any person, entity or public body within or outside of Uganda who collects, processes, holds, or uses personal data belonging to a Ugandan citizen.

Principles under the DDPA

1. Accountability
2. Lawfulness and fairness
3. Adequacy, relevance and minimisation
4. Data retention limit
5. Quality of data
6. Transparency and participation
7. Security safeguards

Conclusion

- The Personal Data Protection Office has embarked on enforcement measures.
- Likely enforcement challenges may include the varying systems and technological advances.
- Data subjects may face an evidentiary burden, e.g. internet, social media, often render “personal data” “public information”.
- Proper documentation of the sources of data and the categories of data held is crucial.



Compliance obligations for data collectors, controllers and processors

Presentation by **Stella Nakazibwe**
Senior Associate, Tax & Legal Services
PwC Uganda

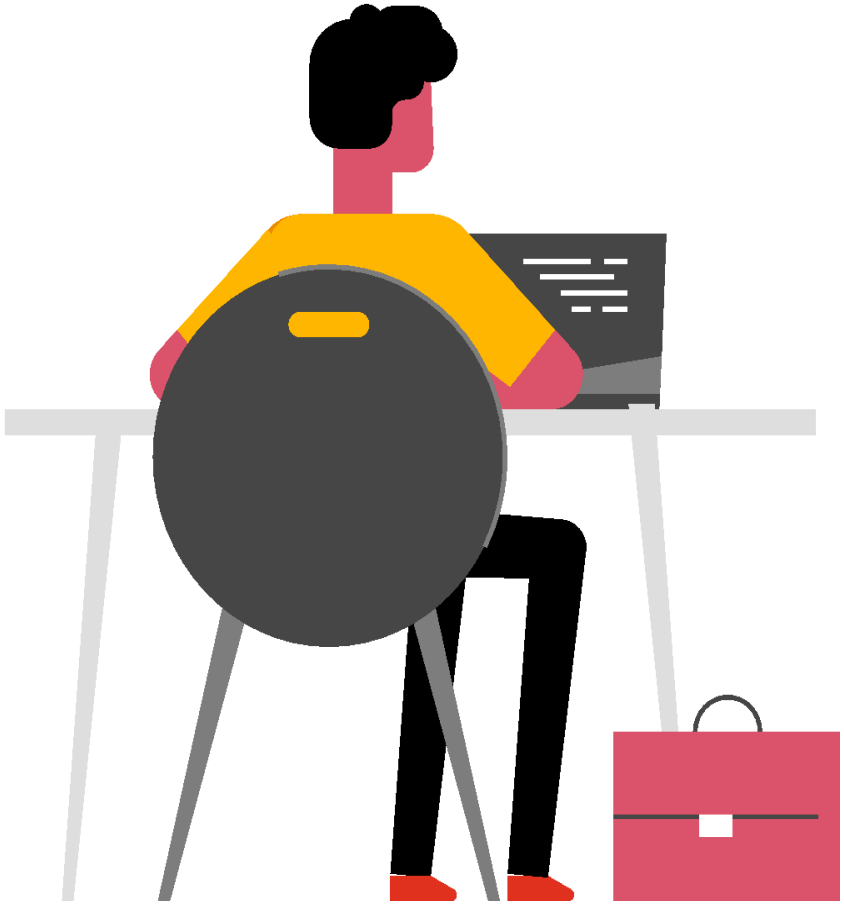
Introduction

Key definitions:

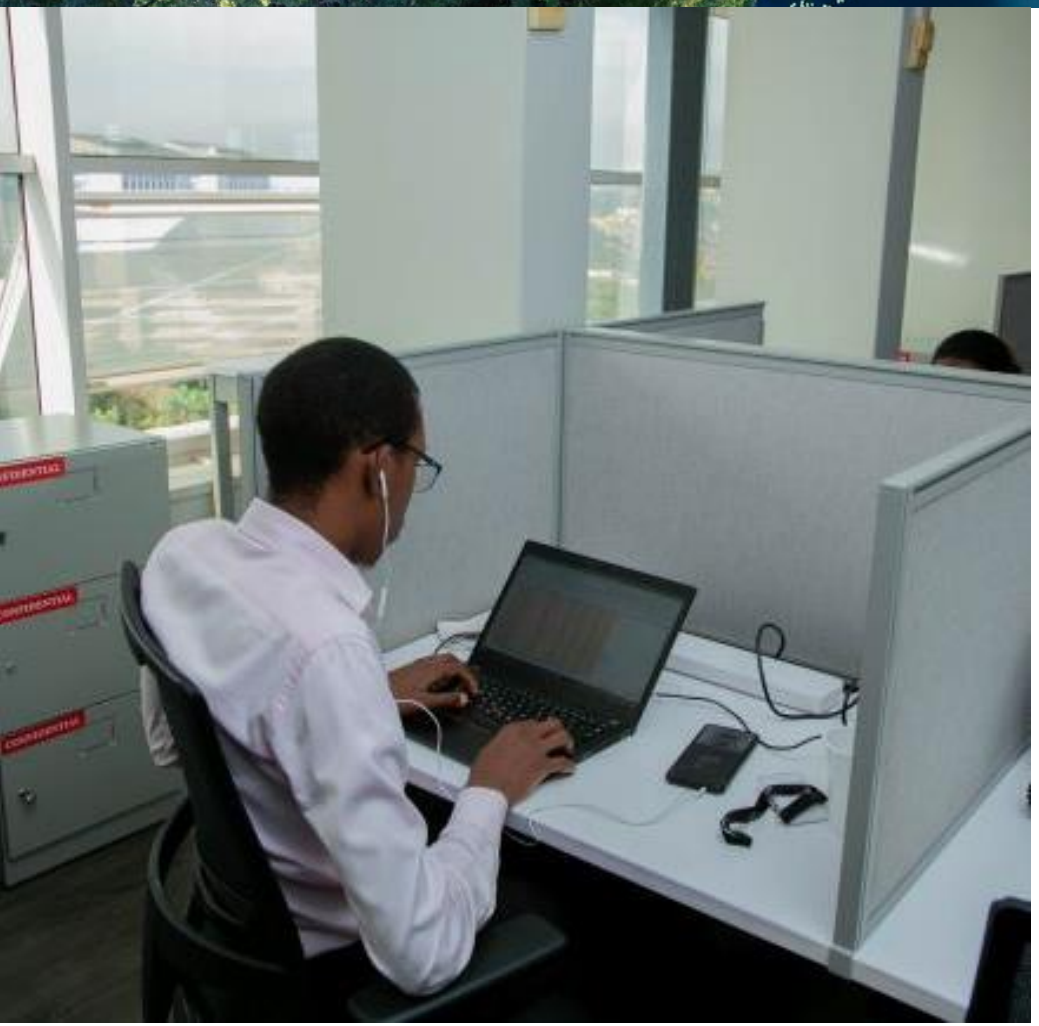
- Data is information processed, recorded or forms part of an accessible record.
- Information- data, text, images, sounds, codes, databases stored in any format.
- A data subject is an individual from whom personal information is collected.
- A data collector is one who collects data.
- A data controller determines the purpose and manner in which data is processed; and
- A data processor is a person who processes data on behalf of the data controller

Obligations set out in the law

- Consent from the data subject before personal data is collected.
- Prohibition on collection and processing of special personal data.
- Prohibition on collection of personal data relating to children.
- Limitation on processing personal data outside Uganda.
- Adhering to the rights of data subjects.
- Deletion or de-identification of data and best practices.
- Appointment of a data protection officer.



Registration with NITA-U



- NITA-U is mandated to maintain a register of all persons collecting or processing personal data and the purpose for its collection.
- Registration applies to all organisations/ persons that collect, process and control personal data.
- This is an online application process completed upon payment of fees.
- Every organisation may either have an information security/ data privacy policy at time of registration or provide its security measures.

Registration process cont...

- NITA is required to review and respond to application within 30 days and notify applicant within the next 15 days.
- Once registration is approved, a Certificate of Registration will be issued.
- Registration is valid for 12 months from the registration date and must be renewed annually.
- A registered entity must maintain updated records and notify NITA-U of any change in its registered particulars within 14 days of the change.

Annual Compliance Requirements

Every registered data collector or processor or controller is required within 90 days after the end of every financial year to submit to the PDPO;

I. a summary of all complaints received and how they have been resolved; and

II. all data breaches and the action taken to address them.

Role of the Data Protection Officer

The DPO is reponsible for the following:

1. Conducting regular assessments and audits to ensure compliance;
2. Acting as the point of contact between the organization and NITA-U;
3. Maintaining records of all data processing activities conducted by the organisation;
4. Responding to data subjects' inquiries and security measures to protect their personal data; and
5. Ensuring that data subjects' requests to see copies of their personal data or to have their data erased are fulfilled as necessary.

Rights of data subjects

1. Right to access

The data controller is expected to comply to a request to access information within 30 days.

2. Right to erasure

Personal data should be erased if it is no longer needed for its original purpose, on withdrawal of consent and upon data being processed unlawfully.

3. Right related to automation

Right to receive notices in respect of automated decisions taken on behalf of the controller, and also a right to require the data controller to reconsider decisions taken by automated means.

4. Right to object processing;

Data subject may object to processing personal data which causes or is likely to cause unwarranted substantial damage to the data subject. The data controller must comply to this request within 14 days.
For every notice to the data-subject which gives reasons of non-compliance, a copy of the same must be given to NITA-U.

5. Right to rectification of inaccurate data

Controllers must ensure that inaccurate data is rectified and amended for it to be adequate for a specific purpose.

6. Right to information

Right to information that describes the relationship with the controller i.e contact details, reasons for processing the personal data and legal basis. This also relates to informed consent.

7. Right to restrict processing of data for direct marketing

A data controller may be notified to stop processing data for direct marketing. However, an agreement can be signed for pecuniary benefits.

Notification of security breaches

NITA should be notified immediately where personal data has been accessed or acquired by an unauthorized person.

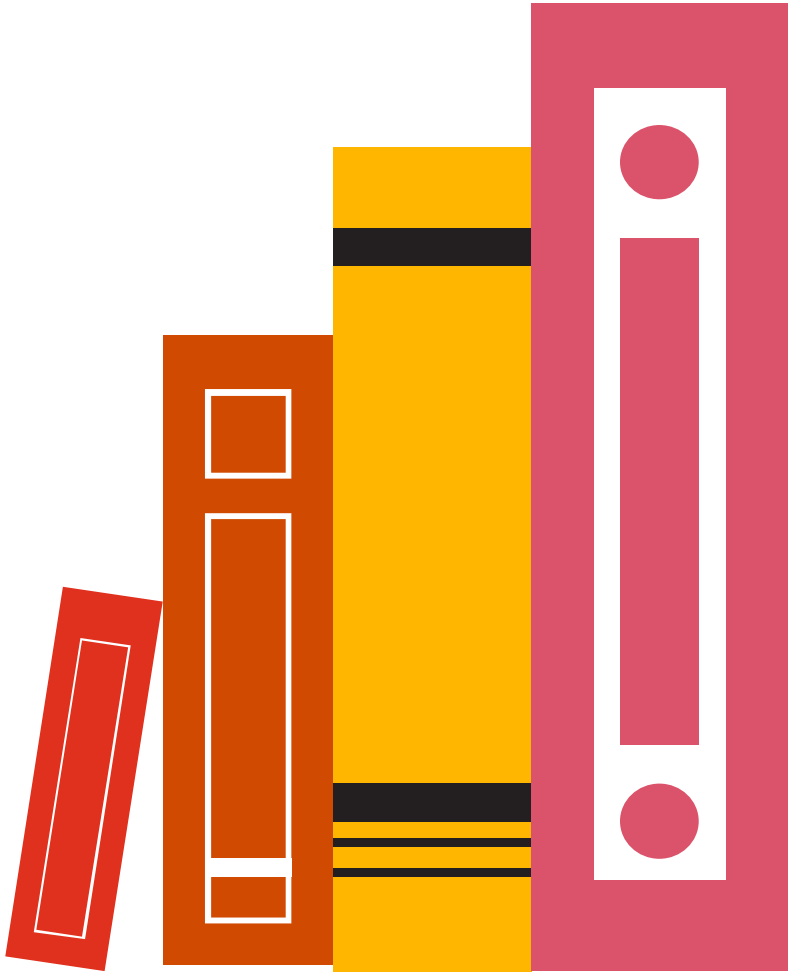
The notification should include the nature of unauthorized access or acquisition and the remedial action which has been taken.

NITA-U will review and decide whether the data subject should be notified of the breach and how information should be relayed to the data subject. Data subject must receive sufficient details to enable them take protective measures against the consequences of unauthorized access or acquisition of their data.

NITA-U may direct the organisation to publicise the fact of the compromise to the integrity or confidentiality of the personal data if it has grounds to believe that publicity would protect a data subject who is affected by the unauthorised access or acquisition of data.

A data subject has a right to lodge a complaint to the data protection office at NITA-U upon violation of their rights. The data subject is entitled to compensation for damage and distress caused by the failure of a data controller to comply with the Act.

What can you start doing to be more compliant?



- Ensure both manual and electronic systems have adequate security measures for storage, encryption and automated deletion when not required.
- Appoint a DPO and empower them to enforce compliance within the organisation.
- Obtain explicit consent for all personal data being collected and processed.
- Train staff to help them understand obligations, rights and risks impacting on the business.
- Ensure third parties (suppliers, contractors and partners) have safeguards to protect personal data from both internal and external risks.

Conclusion

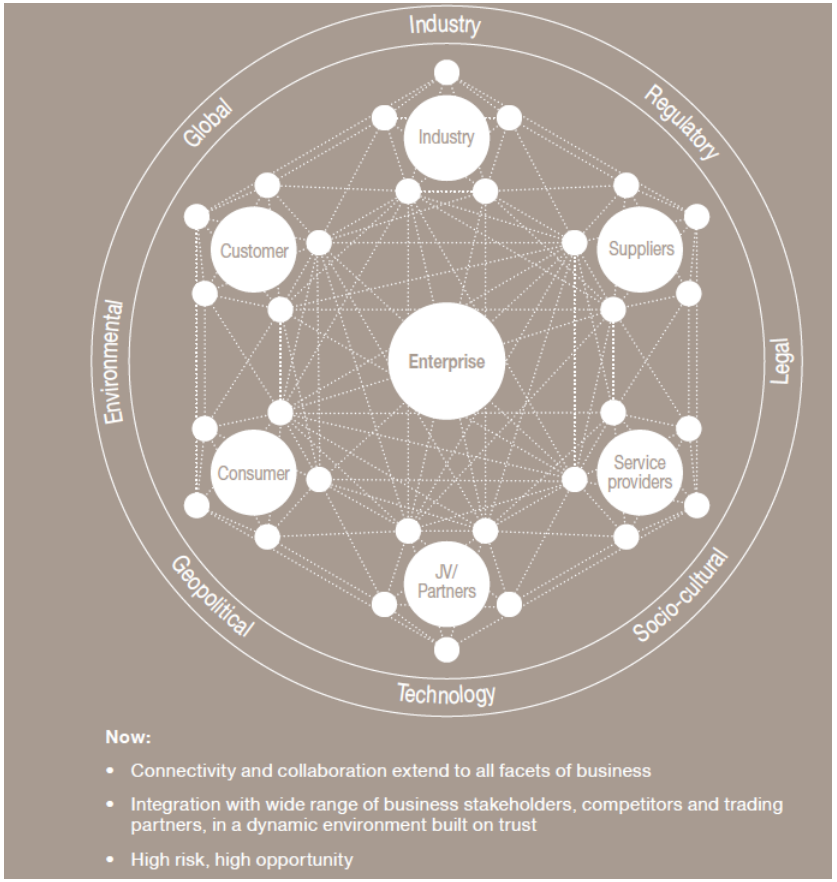
Conducting reviews regularly will help your organisation understand your compliance levels and address potential risks early.

Information security management in light of data protection and privacy laws

Presentation by **Peter Ojekunle**
Senior Manager, Digital Trust and Cyber Security
PwC Uganda

Bringing it all together with a framework

The digital age means that we are now more connected digitally and operate in a data-driven world….



01 Data Privacy Framework

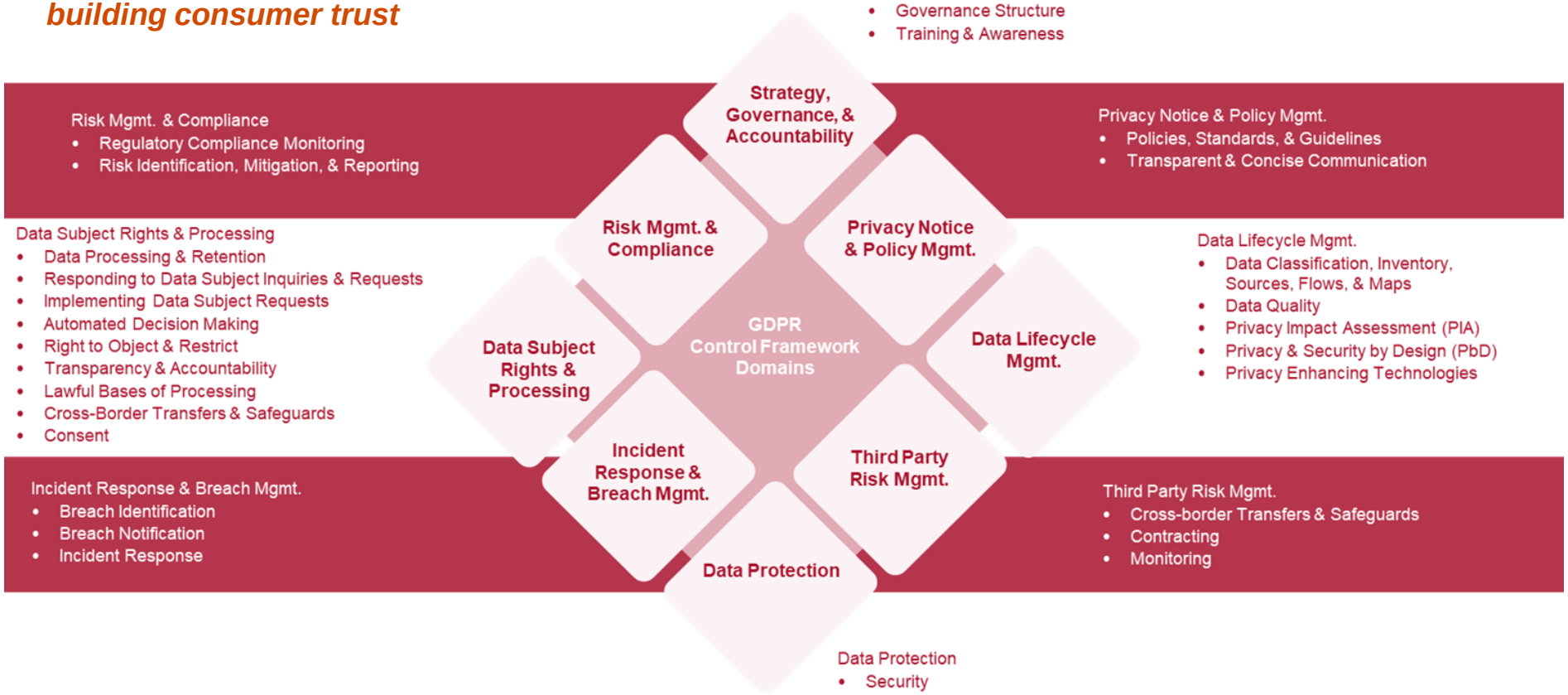
02 Proper integration with ISMS & TPRMS

03 Build Stakeholder confidence and trust

04 Drive a competitive edge

Bringing it all together with a framework

A framework that drives an advantage beyond compliance…. building consumer trust



Conclusion

Strengthening cybersecurity “at all levels — from those who collect data, to those who transmit it, process it, store it, and use it—will be crucial” for personal data protection

THE DATA PROTECTION AND PRIVACY ACT, 2019

Angella Tugume
Manager Data Protection Affairs

March 2022

WHY THE LAW?

Uganda enacted the Data Protection and Privacy Act in 2019 to:

- give effect to Article 27 of the Constitution by safeguarding personal data collected and processed.
- comprehensively and adequately provide for matters on data protection and privacy that were not addressed in the previous legal regime on data protection.
- protect the privacy of the individual and personal data; and
- regulate the collection and processing of personal data.

APPLICATION OF THE LAW

1. Territorial scope

Applies to a person/institution/public body collecting and processing personal data within Uganda and outside Uganda in relation to Ugandan citizens' & Residents' personal data.

2. Material scope

Applies to personal data processed by automated or non-automated means if the data is part of a filing system.

REGULATORY MANDATE

The Data Protection and Privacy Act, 2019 provides that the regulatory body for Data Protection and Privacy is the National Information Technology Authority.

However the Act provides that this shall be done through the establishment of the **Personal Data Protection Office (PDPO)** which shall be responsible for personal data protection under the Authority. Section 5(3) further provides that the office in performing its functions under the Act shall not be under the direction or control of any person or Authority.

Affairs of the Independent Office are run separately from the affairs of NITA.

Personal DATA Protection OFFICE

OBLIGATIONS OF DATA CONTROLLER

1. Establish a data protection and privacy governance framework

- Establish and maintain a comprehensive Data Protection compliance program which should include:
- Designating a Data Protection Officer. Publish the contact details of the DPO as part of the privacy notice/policy/statement.
- Training staff involved in personal data processing operations about the Act's requirements and the impact of non-compliance.
- Developing an internal Data Protection Policy and privacy notice.
- Establishing reporting lines

OBLIGATIONS OF DATA CONTROLLER

2. Ensure personal data is processed lawfully

A controller must have a lawful basis for processing personal data. Processing is lawful if one of the following applies:

- The data subject consents to the processing.
- The processing is necessary for:
- performing a contract with the data subject;
- complying with a legal obligation;
- Performance of a public duty by a public body;
- Medical purposes;
- Prevention, detection, investigation, prosecution or punishment of an offence or breach of law.

OBLIGATIONS OF DATA CONTROLLER

3. Further processing/secondary use of personal data collected

A controller generally cannot use personal data for a different purpose than the one it collected the personal data for, unless the secondary use purpose is compatible with the original purpose.

4. Contract with data processors

Controllers should only use a data processor that provides a guarantee to implement appropriate technical and organisational measures to protect the integrity of the personal data.

OBLIGATIONS OF DATA CONTROLLER

5. Embed Data Protection into operations

To demonstrate compliance with the Act, DPP must embed data protection measures into its day-to-day operations by:

- Developing and implementing personal data policies on retention and data security, breach response and management.
- Conducting Data Protection Impact Assessments under certain circumstances, including where the processing is likely to result in a high risk to the rights and freedoms of data subjects.
- Implementing technical and organizational measures appropriate to the risk posed by the processing.

OBLIGATIONS OF DATA CONTROLLER

6. Take steps to facilitate the exercise of data subject rights

Take steps to facilitate the exercise of data subject rights, including:

- Implementing internal policies and procedures to facilitate the exercise of data subjects' rights.
- Review and revise privacy notices/policies/statements or disclosures to ensure that they comply with Section 13 of the Act to provide certain information to data subjects; and
- Clearly communicate the data subject's rights.

CONSEQUENCES

What happens if the collection or processing of personal data does not adhere to the requirements of the Act?

Violating the Act can lead to significant costs and risks for those involved in its collection and processing. The possible consequences include:

- damage to the reputation of the institution;
- fines of up to two percent of the institution's annual gross turnover; and or
- imprisonment of every officer of the institution who knowingly and willingly authorised or permitted such non-compliance with the Act.

Offences & Penalties under the DPPA & Regulations

	Offences	Financial Penalty (Currency Points)	Imprisonment
1.	Unlawfully obtain, disclose, or procure the disclosure to another person of personal data held or processed by a data collector, data controller or data processor.	240	10yrs/both
2.	Unlawfully destroy, delete, mislead, conceal, or alter personal data	240	10yrs/both
3.	Selling or offering for sale personal data of any person	240	10yrs/both
4.	Failure to register with the Personal Data Protection Office	6	3 months/both
5.	Knowingly giving false information in support of an application for registration	6	3 months/both

Offences & Penalties under the DPPA & Regulations

	Offences	Financial Penalty (Currency Points)	Imprisonment
6.	Processing personal data outside Uganda in countries without adequate measures in place for the protection of personal data at least equivalent to the protection provided for by the Data Protection and Privacy Act, 2019	2 for each day the person is in default	3 months/both
7.	Processing or collection of personal data without consent.	3 for each day that the contravention continues	6 months/both
8.	Failure to honour a request to be examined, produce a document, record or article, or furnish a statement in response to a notice issued under Regulation 42.	2 for each day the person is in default	3 months/both
9.	Failure to comply with any notice issued by the Office under the Data Protection and Privacy Regulations	3 for each day the person is in default	6 months/both

How to Register with the PDPO

Log on to www.pdpo.go.ug
Click on Register
Create an account

For the step by step process, please follow this link:
https://www.youtube.com/watch?v=NcKbWASZgRg

Webinar – On compliance beyond Registration with the PDPO on 31 March 2021. You can register in advance here: https://bit.ly/3t8F9zt

Twitter: @pdpoUG
LinkedIn: Personal Data Protection Office (PDPO)

Personal
DATA
Protection
OFFICE

Thank You

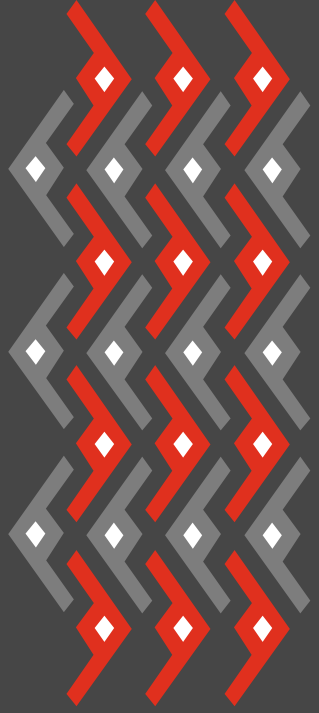
Contact Us

Dorothy Uzamukunda
Manager
Tax & Legal Services
dorothy.b.uzamukunda@pwc.com

Hilda Kamugisha
Manager
Tax & Legal Services
hilda.kamugisha@pwc.com

Peter Ojekunle
Senior Manager
Digital Trust and Cyber Security
peter.s.ojekunle@pwc.com

Stella Nakazibwe
Senior Associate
Tax & Legal Services
stella.nakazibwe@pwc.com



Thank you