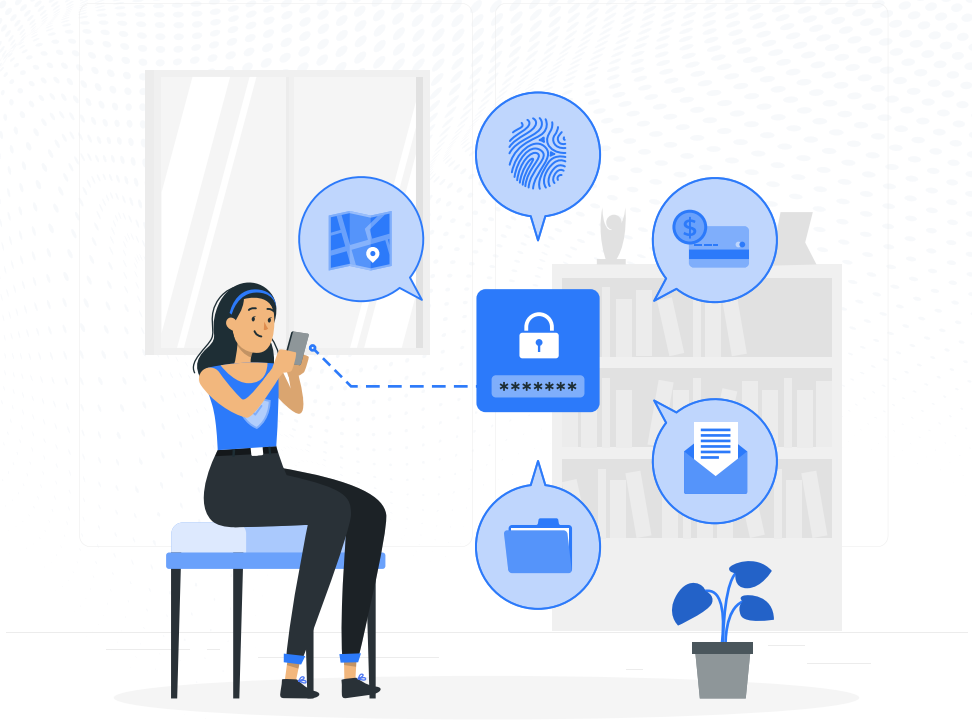
ONYANGO & COMPANY
ADVOCATES, TAX & LEGAL CONSULTANTS

The Data Protection and Privacy Handbook

A starter guide to Data Protection and Privacy Compliance in Uganda

Excellence • Integrity • Passion

Contents



About this Handbook

The data protection and privacy landscape remains intricate as it continuously evolves day by day, presenting a multitude of challenges to organisations. This complexity breeds uncertainty at various levels regarding whether, how, and when to process personal data. Despite the presence of the Data Protection and Privacy Act and its Regulations, organisations in Uganda still grapple with compliance with the diverse provisions and regulatory requirements.

In response to these challenges, we have developed this Data Protection and Privacy Handbook to streamline compliance requirements and facilitate the commencement of your data protection and privacy compliance journey. This toolkit encompasses valuable information and resources aimed at aiding you in evaluating your current business processes in light of data protection and privacy best practices. It equips you with the necessary tools to either enhance your existing practices or ensure alignment with regulatory mandates.

Introduction to Data Protection and Privacy

In Uganda, Data Protection and Privacy is regulated by the Data Protection and Privacy Act Cap 97, complemented by the Data Protection and Privacy Regulations 2021. These legislative frameworks are harmonized with Article 27 of the Constitution of Uganda, which enshrines the right to privacy as a fundamental human right.

The Data Protection and Privacy Act, along with its accompanying Regulations, establish a comprehensive set of compliance obligations and requirements. In the subsequent sections, we will delve into the specifics of these provisions to ensure a thorough understanding of the legal landscape surrounding Data Protection and Privacy in Uganda.

Key Concepts

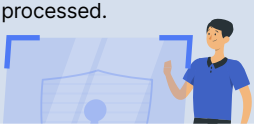
The Data Protection and Privacy Act Cap. 97 and its accompanying Regulations introduce a number of new terms and concepts that are important for you to familiarise yourself with before you can proceed.

Data Collector

is a person who collects personal data.

Data Controller

means a person who alone, jointly with other persons, or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed.



Data Processing

means any operation that is performed upon data by automated means or otherwise.

Data Processor

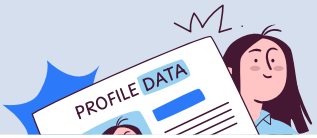
is a person other than an employee of the data controller who processes the data on behalf of the data controller.

Data Subject

means an individual from whom or in respect of whom personal information has been requested, collected, collated, processed, or stored.

Personal Data

means information about a person from which the person can be identified, that is recorded in any form.



Personal Data Protection Office - PDPO

is the office under the National Information Technology Authority-Uganda responsible for personal data protection.

Special Personal Data

means personal data that relates to the religious or philosophical beliefs, political opinion, sexual life, financial information, health status, or medical records of an individual.

Why is data protection and privacy important?

It's very important to protect personal information, maintain individual rights, and prevent any potential harm.
Companies that neglect to ensure the protection of personal data and compliance with data protection and privacy laws in Uganda not only risk penalties but also expose themselves to regulatory intervention, operational inefficiencies, and vulnerability to cyber-attacks, ultimately jeopardizing customer trust.

Reputational damage

Non-compliance with data protection and privacy could tarnish a company's brand and erode the trust of both customers and employees.

Regulatory Intervention

The Personal Data Protection Office (PDPO) may demand documentation and evidence from companies, and in severe cases, may mandate the cessation of processing personal data altogether.

Financial or Criminal Repercussions

The PDPO retains the authority to levy fines against non-compliant entities under Uganda's Data Protection and Privacy Laws. Additionally, these laws stipulate criminal liability for specific instances of non-compliance. The organisation may also face a loss of revenue as a result of data protection litigation.

Operational

Uganda's Data Protection and Privacy Laws grant data subjects increased control over their data, including the right to access, delete, or correct it. Without a clear organizational structure to ensure effectiveness, fulfilling these rights can become an operational burden for organizations.

What is personal data?

Personal data is any information that can be used to identify a person. This information may be recorded in any format.

Examples of personal data

1. Name
2. Contact information such as phone number, and email address, among others
3. Birth certificate, National Identity Card/NIN or Employment ID/No
4. Location
5. CCTV footage
6. Occupation
7. Marital status
8. Level of education
9. Online identifiers such as social media usernames, IP addresses

What is sensitive personal data?

This is personal data that could cause harm to an individual if leaked. The collection of such data is actually restricted under the Data Protection and Privacy Act to circumstances where it's required by the law to collect such data, it's given freely and with consent, or where the collection is for the purpose of legitimate activities of a body or association which is non-profit, among others.

Examples of sensitive personal data

1. Religious or philosophical beliefs
2. Political Opinions
3. Sexual life
4. Financial information
5. Health Status or Medical Records

It is important to differentiate between personal data and sensitive personal data because the processing of sensitive personal data requires an organisation to meet the description provided in the Act as fit to process sensitive personal data.

Data Controller Vs Data Processor

The Data Protection and Privacy Act, along with its Regulations, provide a clear distinction between data controllers and data processors, each bearing distinct responsibilities in safeguarding personal data.

Data Controller

These are individuals or entities who, either independently or jointly with others, determine the purpose and manner in which personal data is processed. A data controller could be an individual, a corporate entity, a charity, or even a government entity.

Examples of data controllers

- A bank collecting personal information from customers to facilitate account opening.
- A hospital collecting personal information from patients for medical purposes
- A government agency collecting personal information from citizens for taxation purposes.
- An educational institution collecting student data for enrolment purposes.

Data Processor

This is an individual other than an employee of the data controller or entity that processes data on behalf of the data controller and in line with the given instructions. Should a processor engage subcontractors for any aspect of data processing, these entities are then designated as data sub-processors.

Examples of data processors

- An agency recruiting personnel on behalf of an organisation.
- A printing company producing identity cards for a corporation.
- A cloud storage provider maintaining personal information on behalf of an organisation.
- A payroll service provider handling salary payments for a company.

Am I a data controller or a data processor?

It is important to recognise that the status of an organisation as either a data controller or a data processor is not fixed; it can vary depending on circumstances and the nature of the personal data being processed.

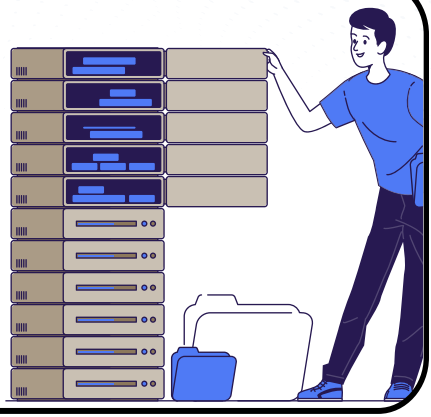
What does it mean if I am a...

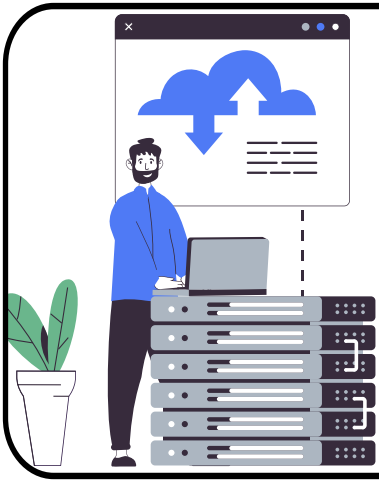
Your responsibilities, obligations, and potential liabilities under the Data Protection and Privacy Act and Regulations hinge upon your role as either a data controller or a data processor.

Data Controller

As a data controller, your responsibilities include; Compliance with data protection principles, upholding individual data protection rights, keeping records of processing operations, enforcing security measures, managing and reporting data breaches, and engaging with data processors that guarantee the protection of personal data.

You are accountable for not only your compliance but also that of your data processors.





Data Processor

As a data processor, your responsibilities include; compliance with the data controller's instructions, taking adequate security measures so as to protect personal data, notifying the data controller of personal data breaches without undue delay, not engaging with any data sub-processor before the data controller's approval, and maintaining a record of all categories of processing activities carried out on behalf of the data controller.

Once you enlist the services of a data sub-processor, you assume responsibility for ensuring their compliance with data protection

What are the rights of data subjects?

These are the individual rights provided under the Data Protection and Privacy Act and intended to give and empower individuals to control their personal data. However, not all these rights are absolute which means some only apply in specific or even reasonable circumstances.

It's important to understand that while individuals possess certain rights outlined above, these rights are not absolute. Organisations also retain the right to reasonably deny certain requests made by individuals seeking to exercise these rights. However, in the event of such a denial, the individual must be promptly notified in writing, providing clear reasons for the decision. This ensures transparency and allows individuals to understand the basis for the denial of their request.

When can you process personal data?

The processing of personal data must adhere to principles of lawfulness and fairness.
Every organisation must establish at least one lawful basis before collecting or processing personal data.

Consent

Processing personal data is permissible when the individual has given explicit consent. In the case of minors, consent must be obtained from their parents or legal guardians.

Legal Authorisation

Organisations may process personal data if required to do so by law or legal mandate.

Necessity

Processing personal data may be necessary for fulfilling a public duty by a public body, ensuring national security, or facilitating the prevention, detection, investigation, prosecution, or punishment of an offense or breach of law.

Contractual Performance

Processing personal data is justified when necessary for fulfilling contractual obligations with the individual, or when taking steps at the individual's request before entering into a contract.

Medical Purposes

It may be necessary to provide adequate medical treatment to a patient.

Legal Compliance

It may be necessary to ensure compliance with legal obligations imposed on the data controller.

It's important to understand that even with a lawful basis, the collection and processing of data must be limited to what is relevant and necessary for the specified purpose. This ensures that individuals' privacy rights are respected and protected.

Principles of Data Protection

The Data Protection and Privacy Act Cap 97 outlines fundamental principles of data protection that must be upheld by both data controllers and data processors when handling personal data. These principles serve as the foundation for the obligations incumbent upon entities involved in the processing of personal data.

Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, ensuring fairness and transparency in all processing activities. Individuals should be informed of how their data is being used and have confidence that it is being handled in accordance with the law. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

Purpose Limitation

Personal data should only be collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes. Any subsequent processing should be compatible with the original purpose for which the data was collected.

Data Minimisation

Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This also requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.

Accuracy

Personal data must be accurate and kept up to date where necessary. Data controllers and processors should take reasonable steps to ensure the accuracy of the data and rectify any inaccuracies without delay.

Storage Limitation

Personal data should only be kept in a form that permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Integrity and Confidentiality

Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, access, alteration, or disclosure. Measures should be in place to safeguard the confidentiality and integrity of the data.

Accountability

Data controllers are responsible for ensuring compliance with data protection principles and must be able to demonstrate such compliance. This includes implementing appropriate technical and organisational measures to ensure and demonstrate compliance, maintaining records of processing activities, and conducting data protection impact assessments where necessary.

By adhering to these principles, you can ensure the lawful, fair, and secure processing of personal data, thereby safeguarding individuals' privacy rights and fostering trust in the handling of personal information.

Steps to ensure effective data protection and privacy compliance

01 Appoint a Data Protection Officer

02 Prepare data protection and privacy policies

03 Establish and Maintain a Personal Data Register

04 Register with the Personal Data Protection Office

05 Respond when individuals ask about their personal data

06 Notify purpose and seek consent

07 Put in place information security mechanisms

08 Manage third parties

09 Notify data breaches

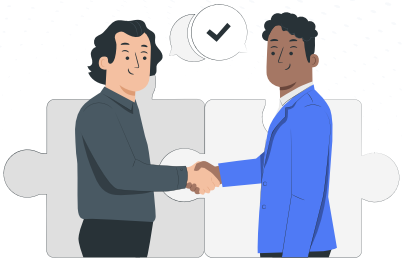
10 Protect personal data when transferring it to other countries

01 Appoint a Data Protection Officer

The Data Protection and Privacy Act introduces the position of a "Data Protection Officer" (DPO) which role is in place to ensure compliance with the Data Protection laws.

Who appoints a DPO?

The Head of an organisation is required to make this appointment. However, the appointment may still be made by any designated member of the organisation's senior management as per the setup within the organisation.



Who could be appointed as a DPO?

This role can be assigned to an existing employee within your organisation or even recruit someone specifically for this role.

The DPO needs to be an expert in data protection, must be independent, adequately resourced, and must report to the highest management level.

What's the role of the DPO?

The DPO assists you in ensuring compliance with the data protection and privacy law, monitoring internal data processing processes, advising on adequate measures, handling inquiries, and acting as a contact person with the Authority.

02 Prepare Data Protection and Privacy Policies

Every organisation is required to have Data Protection and Privacy Policies (DPPPs) in place.

Why are DPPPs important?

DPPPs inform people about your personal data collection and processing activities. They show people you interact with that you take the privacy of their information seriously. You're also required to submit a copy of an Information Security Policy when registering with the Authority.

Why communicate your DPPPs?

The significance of DPPPs can only be realised if those with whom you interact are aware of them. It is, therefore, important to make these policies and procedures accessible to your employees, customers, service providers, third parties, and other relevant stakeholders.

03 Establish and Maintain a Personal Data Register

To safeguard personal data effectively, it is crucial to have a comprehensive understanding of the data collected, and its methods of collection, usage, and storage. This begins with identifying all data processing activities involving personal data within your organisation and maintaining a clear record of how and why such data is utilised. This record, known as a "Personal Data Register," serves as a central repository for documenting and managing personal data processing activities.

What details need to be included in the register?

Consider the following details:

- Name and contact details of your DPO and processor (if applicable)
- The lawful basis and purpose of processing the data.
- A description of the categories of individuals and categories of personal data involved.
- The systems and locations where the personal data is processed.
- Where the data is transferred to and the list of recipients.
- The retention period and enforced technical and security measures.

04 Register with the Personal Data Protection Office

The Data Protection and Privacy Act and Regulations make it a mandatory requirement for every data controller, data processor, or data collector to register with the Personal Data Protection Office (PDPO) at the National Information and Technology Authority (NITA-U).

What obligations arise after registration?

You have a number of obligations including enforcing adequate data security measures, training staff, responding to individual requests, reporting data breaches, conducting data protection risk assessments or audits where necessary, filing a compliance report at the end of the data protection year as well as renewing your registration after twelve (12) months.

05 Respond when individuals ask about their personal data

Individuals have a right to make various requests regarding their personal data, it's therefore the obligation of your DPO to ensure that these requests are responded to.

What should the DPO respond?

The response provided by the DPO is contingent upon the nature of the request and the feasibility of granting it. It is important to understand that these rights are not absolute. The DPO must accurately assess each request and verify the identity of the requester.

Subsequently, the DPO must inform the individual in writing of the decision made regarding their request.

When should the DPO respond?

The timeframe for responding to requests varies depending on the type of request. For example, a request not to process personal data for direct marketing and an objection to the processing of personal data must be responded to within fourteen (14) days while a request regarding automated decision-making must be responded to within reasonable and practicable time.

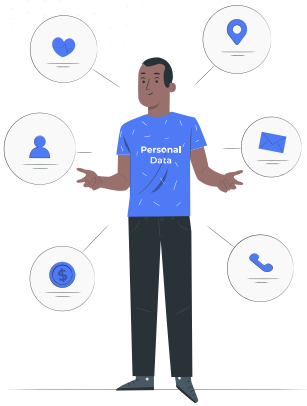
06 Notify purpose and seek consent

Transparency stands as a cornerstone principle within the Data Protection and Privacy Act. It mandates that when collecting individuals' personal data, clear information must be provided to clarify the purpose, nature, and methods of data processing.

What information should I provide?

The following information should be shared with individuals:

- Contact details of your organisation and those of your DPO
- The purpose and lawful basis for processing their personal data
- Categories of personal data to be processed



- Duration for which personal data will be retained.
- Recipients of personal data and details of any cross-border transfers (if applicable).
- Rights individuals possess regarding their personal data.

How Should This Information be provided?

You should provide this information to the individuals at the time of collecting their personal data. You may provide it in writing, orally at the request of the individual, or by electronic means where appropriate. This must be done in a concise, transparent, intelligible, and easily accessible way, in clear and plain language.

What is consent?

Consent means any freely given, specific, informed, and unambiguous indication of the individual's wish which he or she, by a statement or a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her.

How can I obtain consent?

You may make a consent request in writing or by electronic means. The request needs to be in a clear and concise way, using language that is easy to understand, and be clearly distinguishable from any other piece of information such as terms and conditions.
Individuals must be provided with the option to withdraw or refuse consent at any time.

07 Put in place information security mechanisms

The Data Protection and Privacy Act mandates that data controllers, data collectors, and data processors must ensure the integrity of personal data under their control by implementing appropriate, reasonable, technical, and organisational measures. These measures are designed to prevent the loss, damage, unauthorised destruction, unlawful access, or processing of personal data.

Precisely, technical, and organisational measures encompass the functions, processes, controls, systems, procedures, and safeguards implemented to protect and secure the personal information being processed.

Which security measures should I implement?

The security measures to be implemented depend on the size and nature of your organisation, as well as the type of personal data being collected and processed. It may be necessary to engage an information security expert to assess the personal data held by your organisation and determine suitable measures based on potential security risks.

Some common security measures include; physical and digital access controls to restrict access to personal data, controlled admittance to ensure only authorised individuals can access sensitive information, and input controls to regulate the entry of data and prevent unauthorised alterations or additions.

08 Manage third parties

If you engage a third party to process personal data on your behalf, you bear responsibility for their compliance with data protection laws while rendering services for you. It is therefore vital to effectively manage your relationship with these third parties.

Which security measures should I implement?

When establishing contractual agreements with service providers, incorporate clauses mandating their compliance with the provisions of the Data Protection and Privacy Act and Regulations. However, relying solely on contracts may not suffice.

Conduct thorough due diligence to ascertain that third parties have sufficient controls in place to safeguard personal data. Additionally, implement ongoing monitoring procedures to ensure continued adherence to data protection standards by these third parties.

By taking these proactive measures, you can mitigate the risk of non-compliance and protect the personal data entrusted to third-party service providers.

09 Notify Data Breaches

Despite taking all necessary precautions, data breaches can still occur. In the event of a breach, it is a legal obligation to report it to the Authority. Therefore, every organisation must be well-prepared to respond effectively to such incidents.

How to respond to a data breach?

Each data breach requires a tailored response based on the specific circumstances.

However, in general, the following steps should be taken:

- Contain the breach to prevent further compromise of personal data.
- Assess the nature and impact of the breach to determine if it poses a high risk to the rights and freedoms of individuals
- Notify the Authority.
- Conduct a thorough investigation to identify the source of the breach.
- Review the incident and implement measures to prevent future breaches.

How to notify the Authority?

Notification to the authority **must** be made using a specific format (Form 7) and **must** include the following information:

- Details of the breach, including who accessed what, when, and how it occurred.
- Description of the personal data involved in the breach.
- Categories and approximate number of individuals affected.
- Potential consequences of the breach.
- Remedial measures taken or proposed to address the breach.
- Name and contact details of the Data Protection Officer (DPO).

10 Protect personal data when transferring it to other countries

The Data Protection and Privacy Act, along with its Regulations, stipulates that a data controller or data processor based in Uganda, who processes or stores personal data outside Uganda, must ensure that the destination country provides adequate measures for the protection of personal data.

Furthermore, the individual whose data is intended to be processed or stored outside Uganda must provide consent for such transfer to take place. This requirement ensures that individuals retain control over their personal data and are aware of any potential risks associated with its transfer to other jurisdictions.

How Onyango & Co Advocates Can Help...

As experts in Data Protection and Privacy, we are equipped to support your organisation in achieving compliance with Data Protection Laws and Regulations.

Here is how we can assist you:

Compliance Assessment

We conduct comprehensive assessments of your current data protection practices to identify areas of non-compliance and develop tailored solutions to address any shortcomings.

Policy Development

Our team assists in drafting and implementing comprehensive data protection policies and procedures customised to align with your organisation's unique needs and regulatory obligations. This encompasses the creation of essential documents such as privacy notices, cookie policies, privacy policies, and statements.

Training and Awareness

We provide training sessions and workshops for your management and employees to enhance their understanding of Data Protection Laws and best practices, fostering a culture of compliance within your organisation.

Data Subject Rights Management

Our team helps in providing guidance on the establishment of processes for handling data subject requests and ensuring timely and compliant responses to requests for access, rectification, erasure, and other rights under data protection laws.

Data Breach Response

In the event of a data breach, we provide immediate legal guidance and support to help you navigate the breach response process effectively, including notification to the Authority and affected individuals.

International Data Transfers

We advise on the legal requirements and safeguards necessary for transferring personal data across borders, ensuring compliance with applicable data protection regulations. We further advise on the safety of transferring data to particular jurisdictions.

Regulatory Compliance

We provide continuous monitoring and support to ensure ongoing compliance with the Data Protection and Privacy Act and corresponding Regulations, assisting you in mitigating risks and avoiding potential penalties.

Our services encompass various aspects of regulatory compliance, including assistance with registration with the Personal Data Protection Office (PDPO), renewing registration, filing annual compliance reports, and more.

Contract Drafting and Review

We offer expert assistance in drafting and reviewing a wide range of contracts that govern relationships involving the processing of personal data. This includes drafting contracts such as data processor agreements, data sharing agreements, and more, tailored to meet the specific needs and requirements of our clients.

Onyango & Co Advocates can help your organisation navigate the complexities of regulatory compliance and build trust with stakeholders by demonstrating a commitment to protecting personal data.

Meet the Data Protection & Privacy Practice Team

To discuss how we can help you, please get in touch.

Babirye Miriam Kaggwa
Partner

Annet A. Bada
Partner

Onyango Owor
Partner

Namugera Joel Peter
Associate

About Us

Onyango & Co Advocates is a leading law firm dedicated to delivering legal advisory services across different practice areas. Our expertise encompasses Corporate and Commercial Law, Intellectual Property, Banking and Finance, Insurance, Data Protection and Privacy, Employment and Immigration, Tax, Construction and Infrastructure, as well as NGO and Social Enterprise Advisory.

We take pride in our commitment to excellence, providing tailored legal solutions that address the unique needs of each client. We are not just lawyers; we are strategic partners in helping our clients achieve their business objectives.

Contact Us

Plot 182, House B,Bunga-Ggaba Road, Kampala-Uganda

+256(0)701 666 244
+256 (0) 760 255 215

info@onyangoadvocates.com

oc_advocates Onyango and Co Advocates www.onyangoadvocates.com