**Frequently Asked Questions (FAQs)**

1. **What work is the Personal Data Protection Office mandated to do?**

The Personal Data Protection Office (PDPO/Office) is Uganda’s data protection and privacy regulator. It is established as an independent office under the National Information Technology Authority, Uganda (NITA-U) responsible for overseeing the implementation of and enforcement of the Data Protection and Privacy Act of 2019.

The Office is mandated by law to register every person, institution or public body collecting and processing personal data of Ugandan residents.

It also receives and investigates complaints relating to infringement of individuals’ rights under the Data Protection and Privacy Act, 2019;

1. **What is the Data Protection and Privacy Act, 2019 about?**

It is a law enacted to:

1. protect the privacy of the individual and of personal data by regulating the collection and processing of personal information;
2. to provide for the rights of the persons whose data is collected; and
3. obligations of every person, institution and public body collecting and processing personal data.
4. **Whom does the Data Protection and Privacy Act apply to?**

The Data Protection and Privacy Act, 2019 applies to a person, institution or public body –

1. collecting, processing, holding or using personal data within Uganda; and
2. outside Uganda who collects, processes, holds or uses personal data relating to Ugandan residents.
3. **What classifies data as personal data?**

Personal data means information from which a person can be identified. What identifies an individual could be:

* as simple as a name, e-mail address, assigned number; such telephone number, National Identification Number, Tax Identification Number, Social Security Number.
* Or it could be information relating to an individual; such as nationality, age, marital status, educational level qualifications, occupation, behaviour and preferences like internet searches and browser history.

Within personal data there is a category called special personal data which reveals information about an individual that is sensitive that includes the following:

* racial or ethnic origin;
* political opinion;
* religious or philosophical beliefs;
* trade union membership;
* genetic data;
* biometric data;
* health status or medical records;
* sexual life;
* financial information.

Special personal data is sensitive in nature and therefore requires a higher level of protection.

Personal data doesn’t have to be in **written form**, it can also be information about what an individual looks or sounds like, for example **photos** or **audio or video recordings.**

**NOTE:** personal data does not include: any data about a dead person; any information, facts or opinions that do not relate to, or identify people (e.g. employment statistics, company information)**.**

1. **What is ‘processing’?**

Means any operation which is performed upon collected data by automated means or otherwise including –

1. organization, adaptation or alteration of the information or data;
2. retrieval, consultation or use of the information or data;
3. disclosure of the information or data by transmission, dissemination or otherwise making valuable; or
4. alignment, combination, blocking, erasure or destruction of the information or data.
5. **Who is a Data Controller?**

Means a person who alone or 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 or is to be processed.

A controller is the person that decides how and why to collect and use the personal data. This will usually be an organisation, but can be an individual (e.g. a sole trader). If you are an employee acting on behalf of your employer, the employer would be the controller. The controller must make sure that the processing of that data complies with the Act.

1. **Who is a Data Processor?**

In relation to personal data, means a person other than an employee of the data controller who processes the data on behalf of the data controller.

1. **What is a ‘data subject’?**

This is the technical term for an individual from whom or in respect of whom personal data has been requested, collected, collated, processed or stored.

1. **What are the individual’s rights under the Data Protection and Privacy Act?**

1. Right to access personal data.
2. Right to rectification, blocking, erasure and destruction of personal data.
3. Right to prevent processing of personal data for direct marketing.
4. Rights in relation to automated decision-taking.
5. The right to be informed.
6. Right to file a complaint against breach and non-compliance.

Please visit the page on ***“Rights of Individuals under the Data Protection and Privacy Act”*** for more information on these rights and how to exercise them.

1. **What are the obligations of a data controller?**
2. Establish a privacy governance structure, including designation of a data protection officer, as guided by the Regulations.
3. Ensure personal data is processed lawfully and fairly.
4. When intending to further process personal data, data controllers must first verify whether such intended processing is compatible with the purpose for which the personal data was originally collected.
5. Data 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.
6. Embed data protection principles into the data controller’s operations.
7. Develop and implement policies and procedures to enable data subjects exercise their data protection rights.
8. A data controller shall notify data security breaches to the Personal Data Protection Office immediately after becoming aware of it.
9. Any transfer of personal data outside Uganda shall take place only under certain conditions as stipulated by the Act and the Regulations thereunder.

Please visit the page on ***“Obligations of Data Controllers”*** for more information on these obligations.

1. **Do I need to appoint a Data Protection Officer?**

The Act requires persons, institutions and public bodies to designate a data protection officer in the following circumstances where the core activities of the person, institution or public body consist of:

1. the regular and systematic monitoring of data subjects on a large scale; or
2. processing of special personal data.
3. **Are there any consequences for violation or non-compliance with the Act and the Regulations thereunder?**

Breach or violation of the Act and Regulations thereunder can lead to significant costs and risks for those involved. The possible consequences include:

1. damage to the reputation of the person, institution or public body;
2. fines of up to two percent of the corporation’s annual gross turnover; and or
3. imprisonment of every officer of the institution who knowingly and willingly authorized or permitted such non-compliance with the Act.