



UNWANTED WITNESS

"Amplifying Voices, Changing lives"

DATA PROTECTION SELF ASSESSMENT

Introduction

The Data Protection and Privacy Act (DPPA) and the Data Protection and Privacy Regulations (DPPR) came into force on 25th February 2019 and 12th March, 2021 respectively. The DPPA 2019 and DPPR 2021 affect every organization collecting and processing personal information of Ugandans.

This Unwanted Witness comprehensive Data Protection Self-Assessment (DPSA) contains nine (9) key assessment areas to help your organization assess your DPPA 2019 and DPPR 2021 compliance effectiveness. Benchmark your existing processes to identify any missing procedures and controls.

This DPSA seeks to help organizations implement and evaluate the programs and practices necessary to establish accountability for responsible data protection, which will eventually reduce business risk through better data protection planning for their critical business data.

Key Assessment Areas:

1. Lawfulness, Fairness, Accountability and Transparency
2. Consent
3. Data Subjects Rights
4. Accuracy and Retention
5. Transparency Requirements
6. Data Controllers/Processors Obligation
7. Data Protection Impact Assessment
8. Data Security
9. Data Breaches

Lawfulness, fairness, accountability and transparency (Section 3 (a, b, and f))

a. Information audit

You should organize an information audit across your business or within particular business areas. One person with in-depth knowledge of your working practices may be able to do this and will identify the data that you process and how it flows into, through and out of your business. Has your business conducted one?

b. Documentation of Personal Data

Has your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.

c. Lawful basis for processing personal data

There are five (6) available lawful bases for processing personal data. No single basis is better or more important than the others are. The basis that is most appropriate will depend on the purpose for processing and the relationship with the individual. Has your business has identified lawful bases for processing user personal data?

Consent (Section 7 of the DPPA 2019)

- a. Have you reviewed your organization's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of statement or a clear affirmative action?
- b. Is the personal data you currently hold based on consent meet the required standard under the Data Protection and Privacy Act 2019, have you re-sought the individual's consent to ensure compliance with the Data Protection and Privacy Act 2019?
- c. Are procedures in place to demonstrate that an individual has consented to their data being processed?

- d. Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?
- e. Where online services are provided to children, are procedures in place to verify age and get consent of a parent/ legal guardian, where required?
- f. Does your business have systems to record and manage ongoing consent.

Data Subject Rights (Part V of the DPPA 2019)

a. Access to personal data (Section 24 of the DPPA 2019)

Does your business have a process to recognise and respond to individuals' requests Subject Access Requests (SARs) to access their personal data?

b. Right to be informed (Section 13 of the DPPA 2019)

Individuals need to know that you are collecting their data, why you are processing it and who you are sharing it with. Has your business provided privacy information to individuals?

c. Rectification, blocking, erasure and destruction of personal data (Section 28 of the DPPA 2019)

Are there controls and procedures in place to allow personal data to be rectification, blocking, erasure and destruction?

d. Right to prevent processing of personal data (Section 25 of the DPPA 2019)

- i. Are there controls and procedures in place to halt the processing of personal data where a person has on valid grounds sought the prevention of processing?
- ii. Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?

e. Rights in relation to automated decision-taking (Section 27 Section)

- i. If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected?
- ii. Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision?

Accuracy and Retention (Section 18 of the DPPA 2019)

a. Data minimization (Section 14 of the DPPA 2019)

Is the personal data collected limited to what is necessary for the purposes for which it is processed?

b. Quality of Information (Section 15 of the DPPA 2019)

Are procedures in place to ensure personal data is kept up to date, complete and accurate and where a correction is required, the necessary changes are made immediately?

c. Retention

- i. Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected?
- ii. Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies?

Transparency Requirements (Section 3 (f) of the DPPA 2019)

a. Transparency to customers and employees (Section 3 of the DPPA 2019)

- i. Do your customers/employees fully participate in the collection, processing, use and holding of their personal data?

- ii. Where personal data is collected directly from the individuals, are procedures in place to provide the information listed in Section 13 of the DPPA 2019?
- iii. If personal data is not collected from the subject but from a third party (e.g. acquired as part of a merger) are procedures in place to provide the information listed at Section 13 of the DPPA 2019?
- iv. When providing a service or sale of a good, are procedures in place to proactively inform individuals of their rights?

Data Controller Obligations (Part III of the DPPA 2019)

a. Accountability (Section 3 (a) of the DPPA 2019)

Does your company have Personal Data processing agreements with suppliers and other third parties processing personal data on your behalf?

b. Data Protection Officers (DPOs) (Section 6 of the DPPA 2019)

- i. Has your organization appointed a DPO as per Section 6 of the DPPA 2019?
- ii. Where a DPO is appointed, are escalation and reporting lines in place? Are these procedures documented?
- iii. Have you published the contact details of your DPO to facilitate your customers/ employees in making contact with them?

Data Protection Impact Assessments (DPIAs) (Regulation 12 of the DPPR 2021)

- a. Does your company have a process for identifying the need for, and conducting of, DPIAs?
- b. If yes, are these procedures documented?

Data Security (Section 20 of the DPPA 2019 and Part VII of the DPPR 21)

- i. Has your company assessed the risks involved in processing personal data and put measures in place to mitigate against them?
- ii. Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?
- iii. Is there a documented process for resolving security related complaints and issues?
- iv. Is there a designated individual who is responsible for preventing and investigating security breaches?
- v. Does your business have entry controls to restrict access to premises and equipment in order to prevent unauthorized physical access, damage and interference to personal data?
- vi. Does your business have established controls to manage the use of removable media in order to prevent unauthorized disclosure, modification, removal or destruction of personal data stored on it?

Data Breaches (Section 23 of the DPPA 2019)

a. Data security breaches and response obligations (Section 23 of the DPPA 2019)

- i. Does your organization have a documented privacy and security incident response plan?
- ii. Are plans and procedures regularly reviewed?
- iii. Does your business have a procedure in place to report a breach to the Personal Data Protection Office and to affected individuals, where necessary?
- iv. Are there procedures in place to notify data subjects of a data breach (where applicable)?

- v. Are all data breaches fully documented?
- vi. Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches?

b. International data transfers (Section 19 of the DPPA 2019)

- i. Do you transfer your customer's/ supplier's/ employee's personal data outside Uganda?
- ii. Does this include any special categories of personal data?

c. Transparency

Are data subjects fully informed about any intended/ shared information with third parties or Government?