

Data Governance and Data Privacy Considerations

In a digital world, organisations gather and treat vast amounts of information regarding people, customers, employees, students, patients and other stakeholders. Thus, it is crucial for data to be accurate, secure, in responsible hands and utilised for legitimate purposes, and data governance and data privacy are essential to this.

In Uganda, one of the key laws dealing with personal information is the Data Protection and Privacy Act, 2019 (Act No. 9 of 2019). It governs the processing, collection, retention and utilisation of personal data and sets rights for persons and duties for organisations with regard to the processing of their personal data.

WHAT IS DATA GOVERNANCE?

Data governance is the framework of policies, procedures, standards, roles and responsibilities used to manage data.

Key concerns:

- Data ownership and accountability
- Data quality and accuracy
- Data security and access control
- Data privacy and compliance
- Data retention and disposal
- Data lifecycle management

WHAT IS DATA GOVERNANCE?

Data governance answers questions like:

- Who owns the data?
- Who is accountable for its quality and security?
- What rules govern how it can be used?
- How is compliance monitored and enforced?

Data privacy

Data privacy is a subset of data governance concerned specifically with the appropriate handling of personal data — information that can identify a living individual (a "data subject").

While governance is about control and stewardship broadly, privacy is about protecting individual rights over personal information.

Data Governance vs. Data Privacy

DATA GOVERNANCE	DATA PRIVACY
Broad management framework for ALL organizational data	Focused specifically on PERSONAL / identifiable data
Concerned with quality, accessibility, and security	Concerned with individual rights and consent
Defines who owns data, who is accountable, and how it's used	Protects the data subject, not just the data itself
An internal management discipline	Often a statutory / legally mandated obligation

Why Data Privacy Law Matters

- **Rapid Digitization.** Mobile money, e-government, fintech, and health records collect personal data at unprecedented scale.
- **Real Risks of Breaches.** Financial loss, identity theft, reputational harm, and erosion of public trust follow mishandled data.
- **Cross-Border Complexity.** Cloud storage, outsourcing, and multinational platforms create jurisdictional challenges.
- **Global Convergence.** Many national laws including Uganda's draw on frameworks like the EU's **General Data Protection Regulation**.

UGANDA'S DATA PROTECTION & PRIVACY ACT, 2019

- The Act was assented to by the President on 28 February 2019 and commenced on 1 March 2019. It gives effect to Article 27(2) of Uganda's Constitution, which protects the right to privacy specifically that no person shall be subjected to interference with the privacy of their home, correspondence, communication, or other property.
- The Act's stated objective is to protect individual privacy by regulating the collection and processing of personal information both within Uganda and, where the data relates to Ugandan citizens, outside Uganda as well, while also establishing the rights of data subjects and the obligations of data collectors, processors, and controllers.

Scope of Application

- Within Uganda. Any person, institution, or public body collecting, processing, holding, or using personal data within Uganda.
- Outside Uganda. Persons outside Uganda who collect, process, hold, or use personal data relating to Ugandan citizens — extraterritorial reach.

Key definitions

- **Data subject.** The individual to whom personal data relates.
- **Data collector.** A person who collects personal data.
- **Data controller.** A person who determines the purpose and manner of processing.
- **Data processor.** A person who processes data on behalf of a controller.
- **Consent.** Any freely given, specific, informed, and unambiguous indication of the data subject's wishes, signified by a statement or clear affirmative action, agreeing to the collection or processing of their personal data.

The Seven Principles of Data Protection

- Lawfulness and specificity of purpose
- Adequacy, relevance, and non-excessiveness of data collected
- Accuracy and being kept up to date
- Retention only as long as necessary
- Processing in accordance with the rights of data subjects
- Adequate security safeguards
- No transfer outside Uganda without proof of adequate protection

PURPOSE LIMITATION & DATA MINIMISATION

- Purpose limitation: collect personal data for a lawful, specific and explicitly defined purpose.
- Data minimisation: collect only data that is adequate, relevant and not excessive or unnecessary.

Example:

- If a university collects a student's phone number for academic communication, it should not automatically use it for unrelated marketing.

WHO ARE THE KEY ACTORS?

- **Data subject.** The individual to whom personal data relates.
- **Data controller.** Determines the purposes and means of processing personal data.
- **Data processor.** Processes personal data on behalf of a data controller.
- Example: A university may be a controller while an external service provider processes data on its behalf.

INFORMATION BEFORE DATA COLLECTION

Before collecting personal data, organisations should provide relevant information including:

- Nature and category of data
- Person responsible for collection
- Purpose of collection
- Whether providing data is mandatory or discretionary
- Consequences of not providing it
- Recipients of the data
- Rights to access and request rectification
- Intended retention period

Rights of data subjects

Important rights include:

- Right to access personal data
- Right to request rectification of inaccurate data
- Rights relating to blocking, erasure or destruction in applicable circumstances
- Right to be informed
- Rights concerning automated decision-taking
- Right to complain about breaches/non-compliance

Rules on Collection and Processing

- A person shall collect personal data directly from the data subject.
- Data must be collected for a lawful purpose that is specific, explicitly defined, and related to the functions of the data collector or controller.
- A data controller or processor shall only process personal data that is necessary or relevant.
- Data collectors/controllers/processors must not collect, hold, or process personal data in a manner that infringes on a data subject's privacy.
- Special categories of personal data (e.g., health, religious belief, sexual life) are subject to prohibition or heightened restriction, with limited statutory exceptions.
- Special rules apply to children's data and to processing personal data outside Uganda.

Data security considerations

Technical safeguards:

- Strong authentication and access controls
- Encryption
- Firewalls and endpoint protection
- Secure backups
- Audit logs and monitoring

Data security considerations

Organisational safeguards:

- Privacy and security policies
- Staff training
- Confidentiality procedures
- Incident-response procedures
- Regular audits

Data breaches

A data breach involves unauthorised access, disclosure, alteration, loss or destruction of personal data.

Examples:

- Hacked student database
- Lost laptop containing confidential records
- Email sent to the wrong recipient
- Stolen credentials
- Unsecured cloud storage

Response to data breaches: identify → contain → assess → document → notify where required → correct → prevent recurrence.

Data Protection Impact Assessment(DPIA)

A DPIA assesses privacy risks before high-risk data processing is undertaken.

Ask:

- What data will be collected?
- Why is it needed?
- Who will access it?
- What risks could affect individuals?
- How will data be secured?
- How long will it be retained?
- What happens if an automated system makes an incorrect decision?

Privacy by design

Privacy should be incorporated into an information system from the beginning.

Practical approaches:

- Collect only necessary information
- Build access controls into the system
- Use encryption where appropriate
- Provide clear privacy notices
- Minimise default data collection
- Design secure deletion and retention processes
- Principle: privacy is a design requirement—not an afterthought.

Data retention and disposal

Organisations should establish clear retention schedules.

Questions:

- Why do we need to keep this data?
- How long is it required?
- Is retention required by law or policy?
- Who can access archived data?
- How will data be securely destroyed?
- Do not retain personal data indefinitely simply because storage is inexpensive.

University data governance

Universities process large volumes of personal information:

- Student registration and academic records
- Examination and attendance records
- Staff and payroll information
- Fees and financial information
- Counselling and health-related records
- Research data

Common risks: weak passwords, excessive access, insecure email, lost devices, poor disposal and cyberattacks

Consequences of poor data governance

Possible organisational consequences:

- Regulatory and legal consequences
- Financial costs and penalties
- Reputational damage
- Loss of public/student trust
- Operational disruption
- Increased cybersecurity risk

Consequences of poor data governance

Possible individual consequences:

- Identity theft and fraud
- Stigma or discrimination
- Financial loss
- Unwanted disclosure

Organisational data governance cycle

1. Identify data
2. Classify data
3. Assign responsibility
4. Establish policies
5. Control access
6. Protect and monitor
7. Manage incidents
8. Retain and securely dispose