AIPI

" A Partnership between BITMi and Rwanda ICT Chamber "

GUIDE TO DATA GOVERNANCE FRAMEWORK & LEGAL COMPLIANCE OF RWANDAN DATA PROTECTION LAW

SUPPORTED BY:

Invest for Jobs
Opportunities for Growth in Africa

sequa

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Federal Ministry for Economic Cooperation and Development

IMPLEMENTED BY:

bitmi Bundesverband IT-Mittelstand e.V.

ICT CHAMBER
Connect. Grow. Expand

AIPI

Introduction

In adherence to Rwandan regulatory requirements, companies prioritize robust regulatory compliance within its operational framework and ensures the ethical and legal use of data within the organization. The key Rwandan regulatory compliance requirements include Law No. 058/2021 on the Protection of Personal Data and Privacy:

- Mandates obtaining explicit consent for data collection and processing
- Requires transparent privacy notices
- Grants individuals rights to access, rectify, or delete their data
- Enforces data security measure

This comprehensive guide empowers you to achieve both legal compliance and effective data governance. The guide includes steps required to ensure your organization safeguards personal data responsibly, fosters trust with stakeholders, and avoids costly legal ramifications. By following these best practices, you'll build a strong foundation for data handling that protects both your business and the privacy of individuals

Objectives

- **Ensure Adherence to Data Protection Laws**: The primary objective is to guide companies in understanding and adhering to r Rwanda's Data Protection and Privacy Law (DPP Law). This includes navigating registration processes (if applicable), understanding legal requirements for data processing, and implementing necessary controls to avoid legal penalties.

- **Promote Compliance**: Equip companies with the knowledge and tools to achieve compliance with relevant data privacy laws

- **Minimize Legal Risks**: By providing clear instructions and best practices, the guide aims to help companies mitigate legal risks associated with data breaches, non-compliance with data subject rights, or unauthorized data processing

- **Empower Data Subject Rights:** Educate companies on respecting and facilitating data subject rights regarding access, rectification, erasure, and restriction of processing

- **Build Trust and Credibility:** By demonstrating a commitment to data protection, companies can build trust and credibility with customers, partners, and stakeholders. This can lead to a competitive advantage and stronger brand reputation

- **Optimize Data Management**: Effective data governance helps companies streamline data handling processes, improve data quality and accuracy, and ultimately make better data-driven decisions.

- **Optimizing data usage and value**: Effective data governance allows companies to leverage their data assets more efficiently and extract greater value from them.

Why a company should comply with the law

The compliance will help to safeguard sensitive and confidential information, prevent cyber crimes, enable better database management and affirm the institution credibility

Implementing robust data security measures, as required by the DPP Law, reduces the risk of data breaches. This protects your company from financial losses, reputational damage, and potential legal action.

Demonstrating compliance with data protection laws shows customers you take privacy seriously and are trustworthy. This can enhance the brand reputation of a company and customer loyalty.

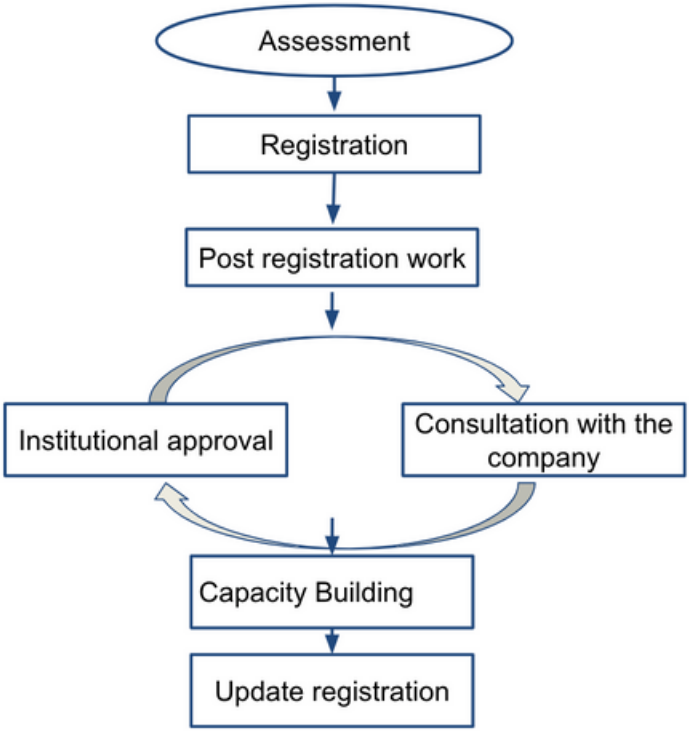
There is a high demand to protect companies from the penalties and legal consequences that may occur in failure to comply with the law as indicated in section 2 of offense and penalties in Rwanda Data protection law on 13th October 2021

Principles

Under the Rwanda's Data Privacy and Protection law which was enforced on 15th October 2023, there are six principles relating to processing of personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Protection of Data Subject rights
- Accuracy
- Storage limitation
- Data minimization

Steps toward compliance



1. Assessment:

1 Identify personnal data

Start by thoroughly identifying all the personal data your company collects, stores, or processes. This includes names, ID numbers, contact information, and any other data that can be used to identify an individual. Companies need to categorize data based on sensitivity. Highly sensitive data, such as health information or biometric data, requires more stringent security measures and may have stricter legal restrictions on how it can be processed.

2 Data mapping

Once identified, map the data where comes from, how it's used, where it's stored, and who has access to it. This creates transparency and helps determine the level of protection needed

2. Registration

Article 29 of Rwanda's Personal Data Protection and Privacy Law1 (hereafter - DPP Law) provides that a person who intends to be a Data Controller or a Data Processor must register with the supervisory authority. Therefore, it is mandatory for any natural person, public or private corporate body intending to be a Data Controller or a Data Processor to register with the Data Protection and Privacy Office under National Cyber Security Authority (NCSA) and receive a registration certificate. Operating without a registration certificate is an administrative misconduct. By registering and providing information about your data processing operations to the supervisory authority, you are making the first step towards compliance and contributing to a responsible, transparent, and accountable data ecosystem in Rwanda.

a)Who can register?

- Any Data Controller and processor who is established or resides in Rwanda and processes personal data while in Rwanda;
- Any Data Controller and processor who is neither established nor resides in Rwanda, but processes personal data of Data Subjects located in Rwanda.

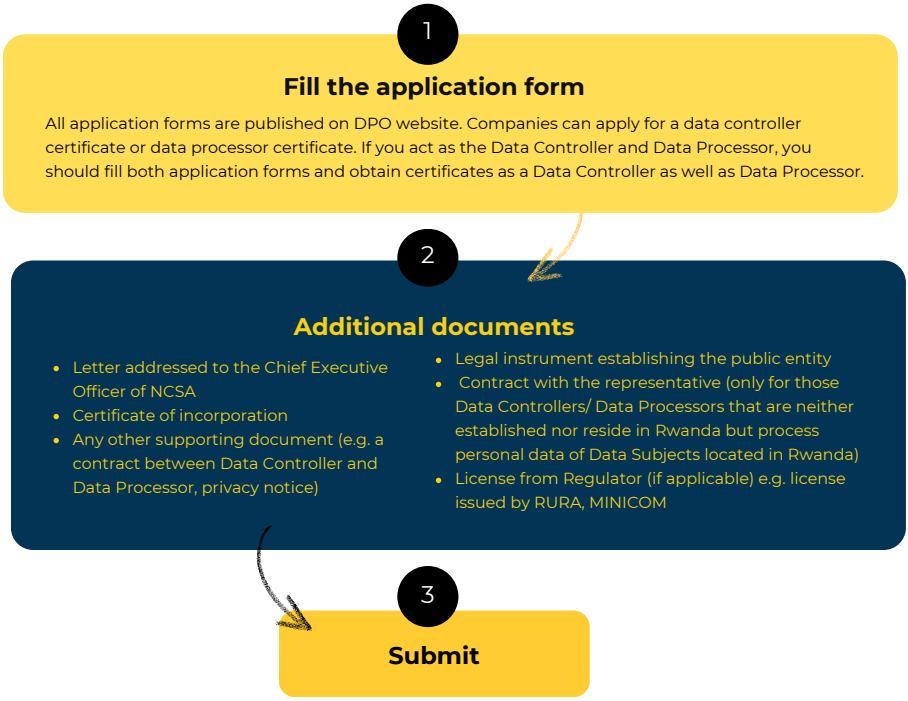
b) Definition of data controller and data processor

- A Data Controller is a natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines the means of their processing. 1 Law N° 058/2021 of 13/10/2021 relating to the protection of personal data and privacy. If your company decides 'why' and 'how' the personal data should be processed, it is the Data Controller.

- **A Data Processor** is a natural person, public or private corporate body or legal entity, which is authorized to process personal data on behalf of the Data Controller. The Data Processor processes personal data only on behalf of the Data Controller. The Data Processor is usually a third party external to the Data Controller and not the Data Controller's employee. This processing is done under the direct instructions of the Data Controller.

There are situations where an entity can be both a Data Controller and Data Processor. For example, if you are a Data Processor that provides services to other Data Controllers, you will likely be a Data Controller for some personal data (for example, in relation to your own employees' data) and a processor for the personal data that you collect or process on behalf of your customer. If you act as the Data Controller and Data Processor, you should fill both application forms and obtain certificates as a Data Controller as well as Data Processor.

c) Registration steps:



Where there is a change in any of the particulars in your application, you must, within fifteen (15) working days of the date of the change, notify the NCSA in writing or electronically of the nature and date of the change. A Data Controller or Data Processor who fails to notify the NCSA will commit a misconduct and will, on conviction, be liable to an administrative fine of not less than two million Rwandan francs (RWF 2,000,000) but not more than five million Rwandan francs (RWF 5,000,000) or one percent (1%) of the global turnover of the preceding financial year.

3. Post registration

Applying for a certificate and obtaining it does not necessarily mean full compliance with the law. While obtaining a certificate may demonstrate a commitment to regulatory requirements, compliance with the law entails adherence to a broader set of obligations beyond mere documentation. It is essential to understand that compliance involves implementing robust policies, procedures, and practices that align with legal mandates and uphold the principles of data protection and privacy. Therefore, while certificates may serve as valuable indicators of compliance, companies must ensure ongoing adherence to legal requirements and best practices to effectively safeguard data subjects' rights and mitigate privacy risks.

A. Gap analysis

aims to identify the gaps or discrepancies between the current state of data protection practices within an organization and the desired state as defined by legal requirements or industry standards. It focuses on assessing the existing policies, procedures, systems, and practices related to data protection to determine areas where improvements or adjustments are needed. It may include interviews, surveys, document reviews, and technical assessments to identify gaps in compliance.

B. Compliance assessment

evaluates the extent to which a company complies with specific legal requirements, standards, or regulations related to data protection. This can involve internal assessments or engaging a qualified data protection professional to conduct an audit. The assessment should look at legal basis for processing data, Data security measures, Data subject rights procedures and Transparency and notification practices.

Outcome: a detailed report outlining areas of non-compliance, weaknesses, or deficiencies in data protection practices as well as actionable recommendations for addressing identified gaps and improving overall compliance with data protection laws.

Outcome: a detailed report indicating the organization's level of compliance with relevant data protection regulations including findings of compliance/non-compliance, areas of improvement, and recommendations for remedial actions to achieve full compliance.

C. Data privacy impact assessment

evaluates the potential risks and consequences associated with the processing of personal data by an organization, considering both the rights of data subjects and the organization's operations. It focuses on assessing the potential impact of data processing activities on individuals' privacy rights, as well as the organization's reputation, finances, and operations. involves identifying and analyzing the types of personal data processed, purposes of processing, data flows, potential risks, and safeguards in place to mitigate risks.
Outcome: a comprehensive report identifying potential risks to data subjects' rights and privacy, as well as recommendations for mitigating those risks. It helps organizations understand the consequences of their data processing activities and implement measures to minimize privacy risks and comply with data protection

D. Designated data owner

A designated data owner is a person who ensures data management practices are in line with the Rwandan Data Protection and Privacy laws. Personal data collected can be subjected to rectification at any time therefore there must be the specific personnel who is in charge of the work of rectification not by any person but this employee is not there

E. Designated data protection officer

Designated data protection officer: should serve as the main point of contact for data protection authorities, employees, and data subjects regarding data protection matters. He ensures compliance with data protection laws and safeguarding the privacy rights of individuals.

F. Data breach response plan

Data breach response plan: outlining procedures for detecting, reporting, and mitigating data breaches. Establish communication channels with relevant authorities and affected individuals to comply with breach notification requirements.

G. Periodic data privacy and protection audits

conduct regular audits and assessments of data processing activities to ensure compliance with the Rwanda Data Protection and Privacy Law. Address any identified non-compliance issues promptly and implement corrective measures

H. Institutional documents, policies and procedure

1.Template for reporting on changes after registration

pursuant to the provisions of the article 32 of the law N° 058/2021 of 13/10/2021 relating to the protection of personal data and privacy in Rwanda states that after receiving a registration certificate, if there is a change in the grounds on which a registration certificate was issued, the data controller or the data processor who received it notifies the supervisory authority in writing or electronically within fifteen (15) working days from the date on which such a change occurred.

2.Data breach response procedure

As corporate body dealing with a number of personal data should have fore predictions of data breach that can happen anytime and get ready in advance by having response procedures in place.

3.Record processed data

or the best practices there must be the procedure of recording each and every processed data within the institution.

4.Sensitive data bank

To have some due distinction between sensitive data and actual personal data there should be treatment in a different manner

5.Guidelines on data protection by design and default

Collecting, processing and storing personal data particularly on sensitive data there must be guidelines to follow to overcome any malfunction that can jeopardize the security of the data.

6.Privacy Notice

This crucial document which ensures the clients that they are going to give their personal data to an institution which sets forth the privacy of personal data in their daily operations, therefore it is important to have in place, specifically the privacy notice has to be published at the website of the company.

7.Consent form for mature people

involved in the collection, processing and storing the data of mature people and as long as, before giving personal data they have to give consent, therefore the consent forms have to be in place by the time of collecting such data

8.Consent withdrawal form

After giving consent to personal data there can be a decision of getting back the consent given, and has to be done in the uniform way as prior one of giving consent

9.Employee Privacy Notice

A company hired, and is still hiring employees and these employees in other words are data subject due to the company holding several personnel, therefore they have to be protected under law as other private individuals by initiating the specific document clarifying the data privacy of employees.

10.Data Retention Policy

Because the data collected by a company has to be retained for a specific period of time, it is in that regard there must be a document specifying the retention policy towards the collected personal data.

11.Data Breach Register

company can face the problem of data breach of the collected data, and it's in that event there must be the register for data breach and measures taken to counter such breaches that can happen in an organization as it is advised by the supervisory authority

12.Data Breach Notification Form to the Supervisory Authority

National cyber security has to get an insight on the data breach that has happen through filling the dedicated form and submitting it

13.Data Breach Notification Form to Data Subjects

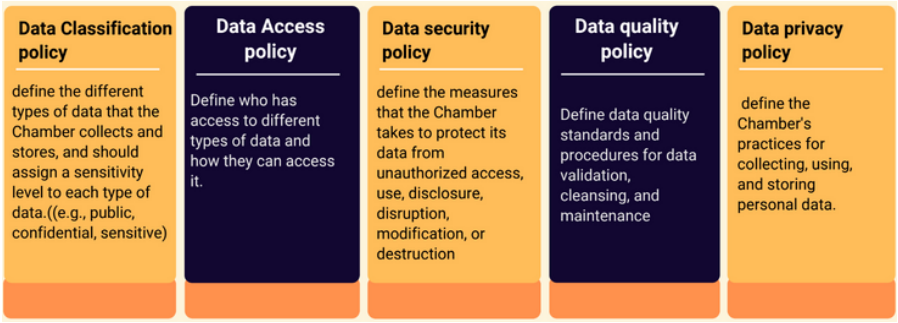
Data subject has to be notified about the breach that has happened to his/her personal data through a form that has to be sent to the due destination of the data subject.

14.Non-disclosure agreement/s

Due to a company having a number of employees who can access the collected personal data, the employees have to sign a non disclosure agreement (NDA).

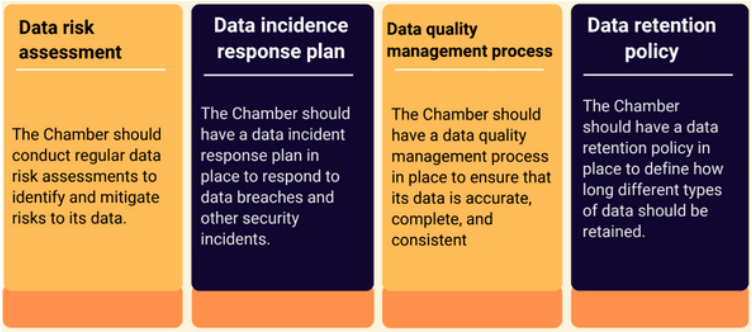
15.Other policies

Create a robust framework that governs how data is handled, ensuring that company maintains the highest standards of data integrity, security, and ethical conduct. Regular reviews and updates to these policies are conducted to adapt to evolving regulatory landscapes and industry best practices. Below are other policies needed:



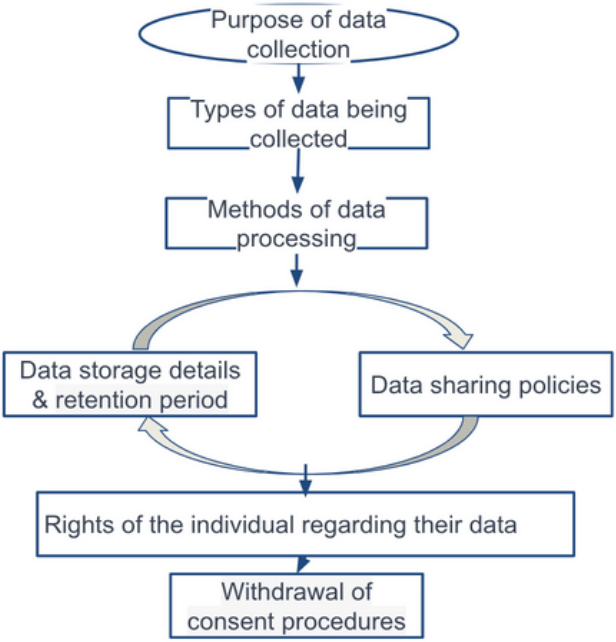
16.Other procedures

Provide step-by-step guidelines on how to execute key data governance activities. Here are essential procedures and processes that support data governance:



17.Consent form

Consent form refers to a document or a formal agreement through which an individual provides explicit permission or authorization for an organization to collect, process, and use their personal data for specific purposes. The main purpose of a consent form is to obtain explicit permission from an individual, allowing an organization or entity to collect, process, and use their personal data for specific purposes. This form serves as a legal and ethical safeguard, ensuring that data processing activities adhere to the principles of transparency, accountability, and respect for individual privacy rights.



Best practices:

- Using of clear and simple language
- Ensuring transparency and clarity in all sections
- Providing options for easy withdrawal of consent
- Include contact information for inquiries and concerns if possible

4. Capacity building

Capacity building of employees is an important step towards achieving compliance with data protection and privacy laws in Rwanda. Here's how organizations can approach this:

Training awareness

- Conduct regular training sessions to raise awareness among employees about the importance of data protection and privacy.
- Educate employees about the provisions of the Rwanda Data Protection Law and their roles and responsibilities in ensuring compliance

Understand legal requirement

- Provide training on the specific legal requirements outlined in the Rwanda Data Protection Law, including data subject rights, lawful processing, data security, and breach notification
- Ensure employees understand the implications of non-compliance and the potential consequences for the organization

---

Role specific training

- Tailor training programs to different job roles within the organization, addressing specific data protection responsibilities and requirements relevant to each role
- Provide specialized training for personnel involved in data processing activities, such as IT staff, HR professionals, and customer service representatives.

Data handling procedures

- Train employees on proper data handling procedures, including data collection, storage, access, sharing, and disposal.
- Emphasize the importance of obtaining consent, maintaining data accuracy, and respecting data subject rights throughout the data lifecycle.

Data security measures and incident response training

- Educate employees on best practices for data security, including password management, encryption, and safe handling of sensitive information.
- Raise awareness about common cybersecurity threats such as phishing attacks, malware, and social engineering scams
- Provide training on how to recognize and respond to data security incidents and breaches promptly.

Compliance culture

- Foster a culture of compliance within the organization by promoting accountability, transparency, and ethical behavior in data handling practices
- Encourage open communication channels for employees to raise concerns, seek clarification, and report potential compliance issues without fear of reprisal

Continuously evaluate and update training materials to address evolving compliance requirements and organizational needs. By investing in the capacity building of employees through comprehensive training, organizations can empower their workforce to understand, uphold, and implement data protection and privacy principles effectively.

Data Governance

Implementing a data governance program is essential for a company. It provides a structured framework to ensure the quality, accuracy and security of data, the operating model, roles and responsibilities as well as compliance with data protection regulations. The data governance program helps to mitigate legal risks and safeguard the chamber's reputation.

1.Benefits of Data Governance

- Improve the understanding and quality of data
- Ensure data security, data privacy, and compliance
- Create clear roles and responsibilities within the organization while simultaneously fostering a "data culture
- Produce complete and high-quality data
- Allow accessibility to more data
- Improve data analytics capabilities

2. Data governance framework

This Data Governance Framework is a fundamental component that drives the responsible and strategic data management practices of a company. By aligning its framework with the vision, mission, and strategic objectives, company ensures that its data-related activities directly contribute to the chamber's broader goals. This alignment fosters a cohesive relationship between data management practices and the strategic direction of the company, enhancing overall effectiveness and supporting sustainable growth.

Data governance framework

3. Data governance roles and responsibilities

The roles and responsibilities within the data governance framework are crucial for effective management of information and technology-related assets. Here's a breakdown of key roles and their respective responsibilities:

a) **Data custodian:** are responsible for the physical storage and security of data, like managing databases and servers. They implement and maintain technical controls set by the data steward to safeguard data access and prevent unauthorized modifications. Other responsibilities:

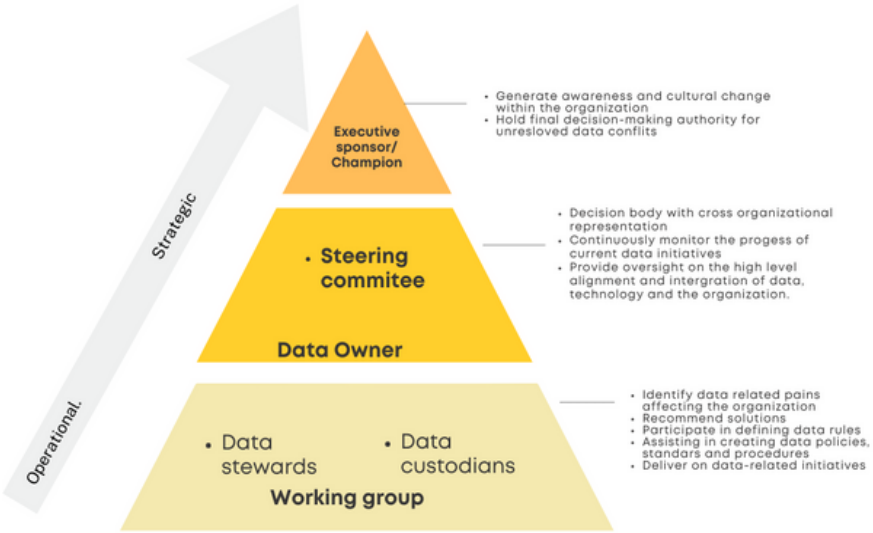
- Oversees data access and storage
- Identifies data stewards for various data domains and collaborates with them on data quality issues
- handle the technical aspects of data storage, versioning master data, and setting up system backups and a disaster recovery plan. They also handle staffing requirements for data governance teams.

b) **Data owner:** who is accountable for the governance of specific sets of data that relate to the functional area within which they operate. The data owner understands the purpose or goal of the data and is accountable for ensuring the quality and correctness of the data and mitigating any risks to the data. The data owner is responsible for ensuring that data stewards in their area of oversight can fulfill their roles, particularly in respect of metadata management, data understanding and data quality management.

c) **Data Steward** is responsible for data management, data quality, and governance. They ensure data is accurate, consistent, and compliant. The data steward is the subject matter who understands and explains the importance of the information and its use. The data steward also provides insight into the general purposes of the data to the data owner, but will be heavily involved in the intricacies of how these objectives might be realized. Other responsibilities are:

- Helps standardize data definitions, rules, and descriptions
- Helps define access policies and optimize data-related workflows and communication
- help standardize data definitions, rules, and descriptions.
- Defining access policies so that the right users have access to all the data they need instantly.

Data Governance operating model



The above operating model establishes a structured hierarchy that optimizes data management processes. The model will enhance data quality and regulatory compliance as well as will facilitate efficient decision making and resource allocation.This operating model establishes clear roles for data custodians and data steward who are responsible for the day-to-day handling and maintenance of dataset, followed by data owner who are entrusted individual who overseeing all datasets and ensure their quality, security and compliance. Data steering committee takes charge, comprising experts and leaders who guide strategic decisions related to data governance. At the pinnacle, the executive committee holds the ultimate responsibility for setting the overarching data governance vision and aligning it with the organization's broader objectives. This hierarchical structure ensures a systematic approach to data governance, with clear lines of responsibility and accountability, fostering a culture of transparency and efficiency within an organization.

Data quality management

Ensuring high quality of data created and used are among the primary objectives of data governance. The data governance program needs to implement procedures to measure, monitor and improve the quality of data by defining data quality rules. Data stewards are responsible for poor data quality. Metrics for data quality need also to be defined.

1. Data quality rules to consider

- **Completeness Rule:** ensures that critical information is not missing from the dataset, promoting a more comprehensive view of data.
- Accuracy Rule: verifies that data values fall within the expected or permissible range, reducing errors and inaccuracies.
- **Consistency Rule:** ensures that data is consistent across different datasets or fields, preventing discrepancies.
- **Uniqueness Rule:** prevents duplicate records and maintains a single, accurate representation of each entity in the dataset.
- **Format Rule:** enforces a standardized format for dates, making it easier to process and analyze the data consistently..
- **Cross-field Validation Rule:** validates relationships between different fields to ensure logical consistency in the data.
- **Default Value Rule:** provides default values for missing or unspecified data, improving consistency and completeness.
- **Conformity Rule:** enforces conformity to standardized naming conventions, promoting consistency in data representation.

2.Data quality metrics to consider:

- Percentage of accurate data entries.
- Percentage of complete data records.
- Time elapsed between data creation and availability.
- Degree of consistency across datasets.
- Percentage of data relevant to current business needs.
- Percentage of data conforming to predefined standards and formats.
- Percentage of duplicate records.
- Accuracy of audit logs.
- Percentage of data meeting security and privacy standards.
- Compliance with established data governance policies.

5. Some tools for data governance

Data governance technology encompasses tools and platforms that help organizations manage and utilize their data effectively. These tools facilitate data quality improvement, ensure data security and compliance, and enable data-driven decision-making. By implementing data governance technology, ICT Chamber can enhance its data management practices and achieve its business objectives.

Data catalog is a centralized repository that provides an organized inventory of data assets within an organization. It serves as a comprehensive index, allowing users to discover, understand, and access available data resources.
Business glossary is a set of definitions and explanations for business terms used within an organization. It ensures a common understanding of terminology across different departments and functions.
A data catalog and a business glossary play complementary roles in managing data assets, providing a foundation for effective data governance, and facilitating collaboration and communication within an organization.

Conclusion

Navigating the landscape of legal compliance and data governance in Rwanda requires a proactive and systematic approach from companies. By adhering to the Rwanda Data Protection Law and implementing robust data governance practices, organizations can safeguard the privacy rights of individuals, mitigate risks associated with data processing, and foster trust among stakeholders. It is essential for companies to prioritize compliance efforts, establish clear policies and procedures, and invest in employee training and awareness. Furthermore, maintaining ongoing vigilance, adapting to regulatory changes, and fostering a culture of compliance are vital for long-term success in data protection and privacy management. Ultimately, by embracing legal compliance and data governance as integral components of their operations, companies in Rwanda can not only meet regulatory requirements but also uphold ethical standards, protect sensitive information, and contribute to a culture of respect for privacy rights and data security.

ICT CHAMBER
Connect. Grow. Expand

info@ictchamber.rw

www.ictchamber.rw

(+250) 781 161 487

AIPI
" A Partnership between BITMI and Rwanda ICT Chamber "

www.aipi.rw

ruanda@bitmi.de

info@aipi.rw

(+49) 241 1890558

(+250) 781 375971

Pascalstr. 6, 52076 Aachen

Fairview Building,
KG 622 Avenue, Kigali