# The Digital Rights in Business Factbook

# TABLE OF CONTENTS

# ACRONYMS

| | |
|---|---|
| **CIPESA** | Collaboration on International ICT Policy for East and Southern Africa |
| **SME's** | Small and Medium Enterprises |
| **DPPA** | Uganda's Data Protection and Privacy Act, Cap 97 |
| **2FA** | Two-Factor Authentication |
| **GDPR** | General Data Protection Regulation - European Union |
| **CCPA** | California Consumer Privacy Act - United States |

# 1 INTRODUCTION


BUILDING DREAMS
- KAMPALA
CREATIVE
HUB UG


# INTRODUCTION

## Purpose and Scope

The Digital Rights in Business Factbook is designed as a practical and accessible guide to support Small and Medium Enterprises (SMEs) in Uganda to understand and navigate the evolving landscape of digital rights, data protection, and cybersecurity. As businesses increasingly adopt digital tools for daily operations, they also take on new responsibilities related to the collection, storage, and use of personal data.

This factbook aims to:

- Simplify complex concepts around digital rights and data protection laws, particularly Uganda's Data Protection and Privacy Act (DPPA), Cap 97
- Provide clear, actionable guidance on how SMEs can protect customer data and secure their digital operations
- Bridge the gap between awareness and practical implementation, enabling businesses to move from understanding risks to taking concrete action

Ultimately, the factbook serves as both an educational resource and a practical toolkit, helping SMEs reduce legal, financial, and operational risks while building more resilient and trustworthy digital businesses.

**119**
SMEs surveyed

**95%**
Youth-led

**82.4%**
Kampala-based

## Context and Relevance

Uganda's SME sector is undergoing rapid digital transformation, with businesses increasingly relying on tools such as social media platforms, mobile money, and online communication channels to engage customers, process payments, and grow their operations. This shift has created new opportunities for market expansion, efficiency, and innovation, particularly among youth-led enterprises.

However, this growth has also introduced significant digital risks. Many SMEs are now handling sensitive customer data, including personal and financial information, without adequate knowledge of how to protect it or comply with existing laws. At the same time, cyber threats such as online fraud, phishing, and account hacking are becoming increasingly common, directly impacting business continuity and customer trust.

**The Data Protection and Privacy Act (DPPA), Cap 97** provides a legal framework to safeguard personal data and define the responsibilities of businesses as data controllers. Despite its importance, awareness and understanding of the law remain limited among SMEs, creating a compliance gap that exposes businesses to potential legal penalties, reputational damage, and financial loss.

In the period between **November and December 2025**, Boundless Minds conducted a survey mapping of 119 youth and women-led small and medium enterprises in the Kampala Metropolitan area. The survey deployed questionnaires (online and physical), aimed at understanding how they use digital tools and protect digital rights in their daily operations.
The factbook will contextualise the findings from the survey, to enhance understanding of digital rights and practices for small/informal businesses.

## Target Audience

This factbook is specifically designed for Small and Medium Enterprises (SMEs) in Uganda, with a particular focus on:

a) Youth-led businesses, which form a significant proportion of the SME ecosystem.
b) Urban and peri-urban enterprises, especially those operating within and around the Kampala Metropolitan Area.
c) Businesses that are digitally active but may have limited access to legal, technical, or cybersecurity expertise.

| Survey Area: | Survey Dates: | Survey Method: | Number of respondents: |
|---|---|---|---|
| Kampala Metropolitan Area | November to December, 2025 | Questionnaires (Online and Physical) | 119 Small-business owners |

## RESPONDENT PROFILE:

- Small and Medium Enterprises (Mostly informal)
- Mostly **1-3 years** operation
- Women-led
- **95%** Youth-led

# 2 UNDERSTANDING DIGITAL RIGHTS AND LAWS

# UNDERSTANDING DIGITAL RIGHTS AND LAWS

## What are Digital Rights?

Digital rights refer to the fundamental rights and freedoms that individuals and businesses have when operating in the digital environment. These rights are essential in ensuring that the use of digital technologies, such as social media, mobile money, and online platforms is safe, fair, and respectful of personal data.

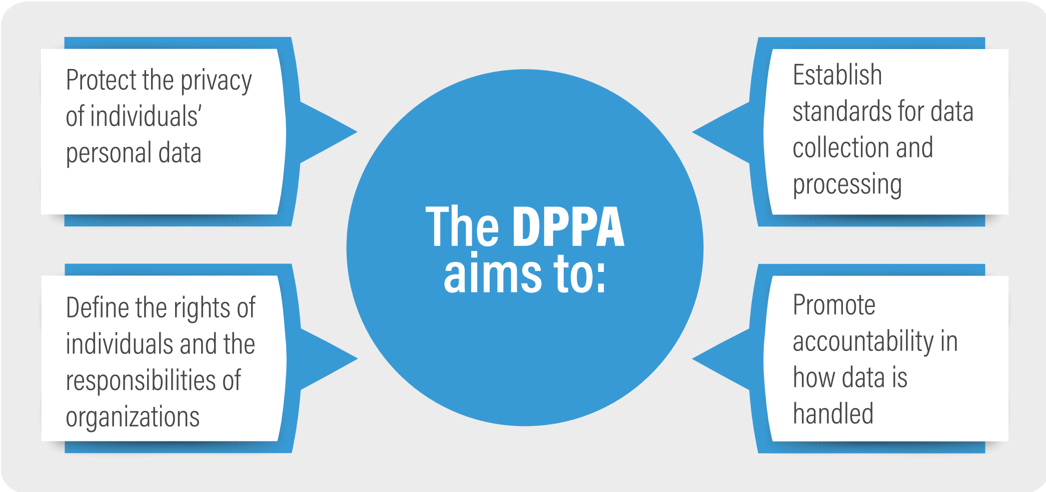
For SMEs, digital rights primarily encompass:

- **Right to Privacy:** Customers have the right to control how their personal information (such as names, phone numbers, and financial details) is collected, used, and shared. Businesses must respect this right by handling data responsibly and transparently.
- **Right to Data Protection:** Personal data must be securely stored and protected from unauthorized access, misuse, or loss. This includes implementing measures such as password protection, encryption, and restricted access.
- **Right to Informed Consent:** Businesses are required to obtain clear and informed consent from customers before collecting or using their personal data. Customers must understand what data is being collected and for what purpose.
- **Right to Digital Safety and Freedom:** Individuals have the right to operate online without being exposed to fraud, harassment, or exploitation. Businesses also have a responsibility to ensure that their platforms and systems do not expose users to unnecessary risks.

## Overview of Uganda's Data Protection and Privacy Act (DPPA), Cap 97

The Data Protection and Privacy Act (DPPA), Cap 97 is Uganda's primary legal framework governing how personal data is collected, processed, stored, and shared. It was enacted to protect individuals' privacy and regulate organizations that handle personal data.

### PURPOSE OF THE DPPA




### KEY ROLES DEFINED BY THE LAW

#### DATA CONTROLLER

A business or organization that determines why and how personal data is collected and used. Most SMEs fall into this category when they collect customer data.

#### DATA PROCESSOR

Any individual or entity that processes data on behalf of a data controller and follows their instructions.
**Examples:** Cloud providers (AWS, Google Cloud), payment platforms (MTN MoMo, Flutterwave), delivery companies, email/SMS services, IT support firms, and CRM/analytics tools.

#### DATA SUBJECT

A data subject is any living, natural person whose personal data is collected, held, or processed by an organization, allowing them to be directly or indirectly identified. This includes individuals such as customers, employees, or website visitors, but generally excludes legal entities (corporations) or deceased individuals.

### RESPONSIBILITIES OF SMES UNDER THE DPPA

**Collect data lawfully and fairly :** Data must only be collected for a specific, legitimate purpose, and customers must be informed.

**Limit data usage :** Data should only be used for the purpose it was originally collected for.

**Obtain consent :** Businesses must get explicit permission from the data subject (the customer, employee, or individual whose data is being collected) before collecting or using their personal data. For children under 18, consent must come from a parent or guardian.

**Maintain data accuracy :** Businesses must ensure that the data they hold is accurate and up to date.

**Ensure data security :** Appropriate measures must be in place to protect data from breaches, loss, or unauthorized access.

**Allow user rights :** Customers have the right to access, correct, or request deletion of their data.

## Legal Requirements for SMEs

According to the Data Protection and Privacy Act, Cap 97 SMEs operating in the  in the digital space must comply with several core legal obligations under the DPPA and general data protection principles:

**a) Data Collection**

- Collect only necessary data
- Clearly explain why the data is needed
- Obtain informed consent

**b) Data Storage**

- Store data securely (e.g., password-protected systems, secure devices)
- Avoid storing sensitive data unnecessarily
- Ensure data is protected from loss or theft

**c) Data Processing**

- Use data only for its intended purpose
- Avoid sharing data with third parties without consent
- Ensure transparency in how data is used

**d) Data Sharing**

- Share data only when necessary and with proper authorization
- Ensure third parties also comply with data protection standards

## Penalties and Risks of Non-Compliance

Failure to comply with the Data Protection and Privacy Act, Cap. 97 (which gives effect to Article 27 of the Constitution of Uganda on the right to privacy) can result in:

- Legal penalties and fines.

**Individuals:** fine up to **245 currency points (UGX 4.9 million)** or imprisonment up to **10 years,** or both.

**Companies:** fines up to **2% of annual gross turnover**, with possible personal liability for directors.

- Reputational damage and loss of customer trust
- Business disruption, especially in cases of data breaches
- Potential legal action from affected individuals (data subjects can sue for compensation for any damage, distress, or violation of their constitutional right to privacy)

For SMEs, even minor violations can lead to significant financial, legal, and reputational consequences, making compliance not just a legal requirement, but a critical business necessity.

## NAVIGATING THE REGULATORY LANDSCAPE

### 1. Local and International Data Protection Regulations

As SMEs increasingly operate in a digitally connected environment, they are not only subject to local laws but may also be affected by international data protection standards, especially when interacting with global platforms, customers, or partners.

### a) Uganda's Legal Framework: The Data Protection and Privacy Act (DPPA), Cap 97

Uganda's Legal FrameworkThe Data Protection and Privacy Act (DPPA), 2019 (Cap. 97) is Uganda's primary legislation governing the collection, processing, storage, and sharing of personal data. It operationalizes Article 27 of the Constitution of Uganda (Right to Privacy).Complementary Laws that SMEs should also be aware of:

- **Electronic Transactions Act, Cap. 99** – Governs electronic contracts, records, signatures, and consumer protection in digital transactions.
- **Computer Misuse Act, Cap. 96** – Addresses cybercrimes, unlawful access to data, and system misuse.
- **Access to Information Act, Cap. 95** – Regulates access to information held by public bodies (with privacy protections).
- **Regulation of Interception of Communications Act, Cap. 101** – Controls lawful interception of communications.

**For SMEs, the DPPA is particularly important because:**

- It applies to any business collecting or handling personal data
- It defines SMEs as data controllers when they determine how and why data is used
- It requires businesses to implement basic data protection and security measures

### b) International Data Protection Frameworks

While SMEs primarily operate under local laws, they may also be indirectly affected by international regulations such as:

- General Data Protection Regulation (GDPR) – European Union
- California Consumer Privacy Act (CCPA) – United States

**These frameworks emphasize:**

- Stronger data protection standards
- Greater transparency and accountability
- Enhanced customer rights over personal data

### Why International Standards Matter for SMEs

- Many SMEs use global platforms (e.g., social media, payment systems)
- Businesses may serve international customers
- Partners or service providers may require compliance alignment

**SMEs must adopt globally acceptable data protection practices, even if they are locally based.**

## COMPLIANCE REQUIREMENTS FOR SMES

To operate legally and responsibly, SMEs must implement practical compliance measures aligned with both local laws (DPPA) and best practices.

## CORE COMPLIANCE STEPS

**01**

**UNDERSTAND LEGAL OBLIGATIONS**
- Become familiar with the DPPA requirements
- Identify what type of data your business collects and processes

**02**

**ESTABLISH DATA PROTECTION PRACTICES**
- Collect data with informed consent
- Store data securely
- Limit data use to specific purposes

**03**

**DEVELOP KEY POLICIES**
- Create a privacy policy
- Define internal data handling procedures
- Establish access control systems

**04**

**IMPLEMENT SECURITY MEASURES**
- Use strong passwords and 2FA
- Regularly update systems
- Protect devices and networks

**05**

**TRAIN STAFF**
- Ensure employees understand data protection responsibilities
- Build awareness of cybersecurity risks

**06**

**PREPARE FOR INCIDENTS**
- Develop a response plan for data breaches
- Know how to report and manage incidents

**49.6%**
of SMEs are unaware of the DPPA

**Majority**
Lack detailed understanding of compliance requirements

**A small portion**
Have formal policies and structured practices

This indicates that many SMEs are operating in **a high-risk, low-compliance environment**

## PENALTIES AND RISKS OF NON-COMPLIANCE

Failure to comply with data protection laws exposes SMEs to significant legal, financial, and operational risks.

**a) Legal Consequences**
- Fines and regulatory penalties
- Legal action from affected individuals
- Enforcement actions by regulatory authorities

**b) Reputational Damage**
- Loss of customer trust
- Negative brand perception
- Reduced customer retention and loyalty

**c) Financial and Operational Impact**
- Loss of revenue due to fraud or system breaches
- Cost of recovering from incidents
- Disruption of business operations

**d) Long-Term Business Risk**

- Difficulty forming partnerships
- Limited access to digital platforms or markets
- Reduced competitiveness

For SMEs, non-compliance is not just a legal issue, it is a business survival risk

**For SMEs, non-compliance is not just a legal issue, it is a business survival risk**

## REGULATORY COMPLIANCE CHECKLIST (FOR SMES)

SMEs can use the following checklist to assess their level of compliance:


### HOW TO USE THIS CHECKLIST

If you answered **"NO"** to multiple questions; **your business is at high risk**
If you answered **"YES"** to most; you are moving **toward compliance and resilience**

# 3 KEY INSIGHTS FROM THE SURVEY DATA

# KEY INSIGHTS FROM THE DATA SURVEY

**40.4%**
of SMEs
Are aware but lack detailed understanding of DPPA requirements

**49.6%**
of SMEs
Have never heard of the Data Protection and Privacy Act

This highlights a critical knowledge gap, where businesses are handling data without fully understanding their legal responsibilities.

## MYTHS VS FACTS

### ON DATA PROTECTION

| MYTHS | FACTS |
| --- | --- |
| Digital rights are only for large companies | All businesses that collect, store, or process personal data are legally responsible under DPPA, Cap 97. |
| Basic precautions are enough | Broader data protection practises are required |
| Compliance is expensive and complex | Basic protections are low-cost or free |
| Nothing has happened yet, thus no risk | Risk is already present with 46.2% SMEs registering incidents |

## DATA PROTECTION BEST PRACTICES

### What is Data Protection?

Data protection refers to the process of safeguarding personal and sensitive information from unauthorized access, misuse, loss, or theft. For SMEs, this includes protecting customer data such as:

| Names and contact details | Identification information | Financial data |
|---|---|---|
| Phone numbers, emails | Photos, IDs | Mobile money details, bank information |

As businesses increasingly rely on digital tools, they become responsible for managing and protecting this data. Effective data protection is not only a legal requirement under Uganda's Data Protection and Privacy Act (DPPA), but also a critical component of business trust, reputation, and sustainability.

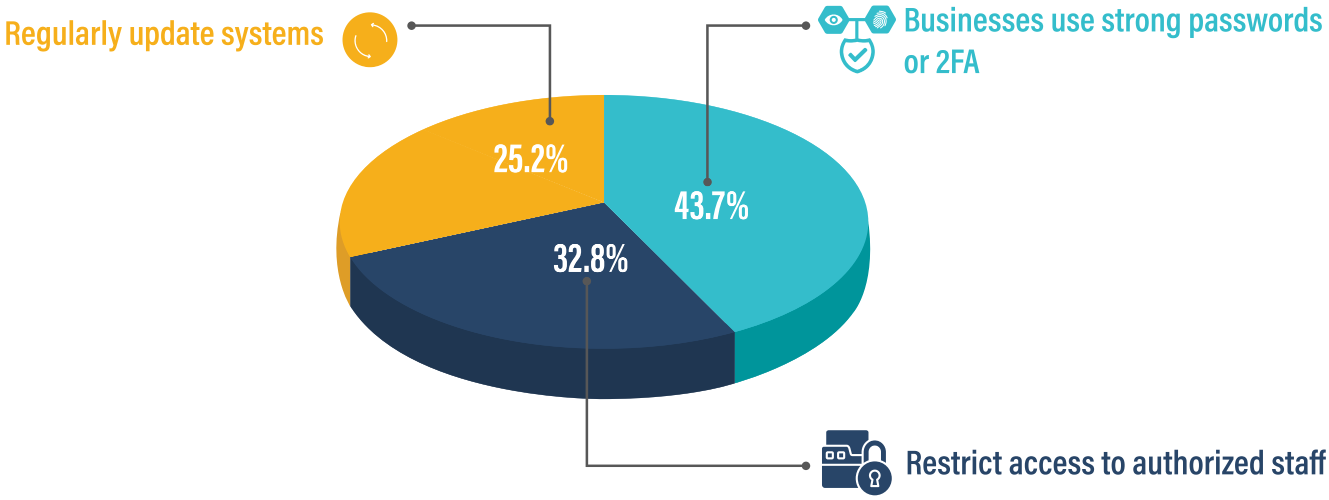
### Poor data protection practices can lead to:

- Data breaches and financial loss
- Loss of customer trust
- Legal penalties and reputational damage

## IMPLEMENTING STRONG DATA SECURITY MEASURES

For tools and resources on **Implementing Strong Data Security Measures**, refer to **CIPESA's Digital Rights and Security Toolkit for Ugandan Businesses,** which explores these tools in detail.

## REALITY CHECK FROM SURVEY DATA




This highlights a significant gap between data handling and data protection practices

### Creating and Enforcing Privacy Policies

A privacy policy is a document that explains how a business:

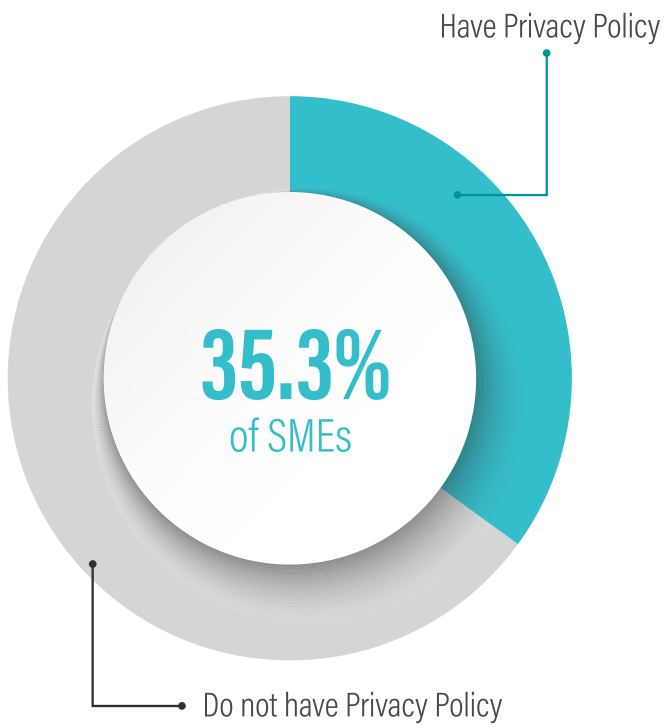
- Collects customer data
- Uses and stores that data
- Protects customer information
- Shares data (if applicable)

### Why Privacy Policies Matter

- They are a legal requirement under data protection laws
- They build customer trust and transparency
- They protect businesses from legal disputes

### What a Good Privacy Policy Should Include

- What data is collected
- Why the data is collected
- How the data is used
- How the data is protected
- Whether data is shared with third parties
- Customer rights (access, correction, deletion)




This means the majority of businesses are operating without formal data protection transparency

# 4 DATA COLLECTION PRACTICES

# DATA COLLECTION PRACTICES

### Data Collection Practices

Best Practices for Collecting Data

- Collect only necessary information
- Clearly explain why the data is needed
- Obtain informed consent before collection
- Avoid collecting excessive or irrelevant data

### Informed Consent

Customers should:

- Know what data is being collected
- Understand how it will be used
- Have the option to agree or decline

### Data Access and Control

Effective data protection requires strict control over who can access information.

**Key Practices**

- Limit access to authorized personnel only
- Use password-protected systems
- Track and monitor access where possible
- Remove access when staff leave or change roles

### Why This Matters

Unrestricted access increases the risk of:

- Internal data misuse
- Accidental data leaks
- Security breaches

### Incident Response and Data Breaches

Despite best efforts, data breaches and cyber incidents can still occur. SMEs must be prepared to respond quickly and effectively.


| 35.3% | Less than half | A big portion |
|---|---|---|
| Of businesses have a privacy policy | Use strong security measures | Lack basic data protection practices |

This indicates that while SMEs are actively collecting data, **data protection maturity remains low**

# 5 CYBERSECURITY AWARENESS AND THREAT MITIGATION


# CYBERSECURITY AWARENESS AND THREAT MITIGATION

## Understanding Cybersecurity Threats

As SMEs increasingly rely on digital platforms for operations, they are becoming more exposed to a wide range of cybersecurity threats. These threats are no longer isolated or rare they are active, frequent, and evolving, directly affecting business continuity, financial stability, and customer trust.

### Common Cybersecurity Threats Facing SMEs

#### a) Online Fraud and Impersonation

This occurs when attackers pose as a legitimate business or individual to:

- Steal money from customers
- Gain access to business accounts
- Manipulate transactions

This is particularly common on social media platforms and mobile money channels, where trust is easily exploited.

#### b) Phishing and Scam Communications

Phishing involves deceptive messages (emails, SMS, or links) designed to:

- Trick users into revealing passwords or sensitive data
- Install malicious software
- Redirect payments to fraudulent accounts

These attacks often appear legitimate, making them difficult to detect without proper awareness.

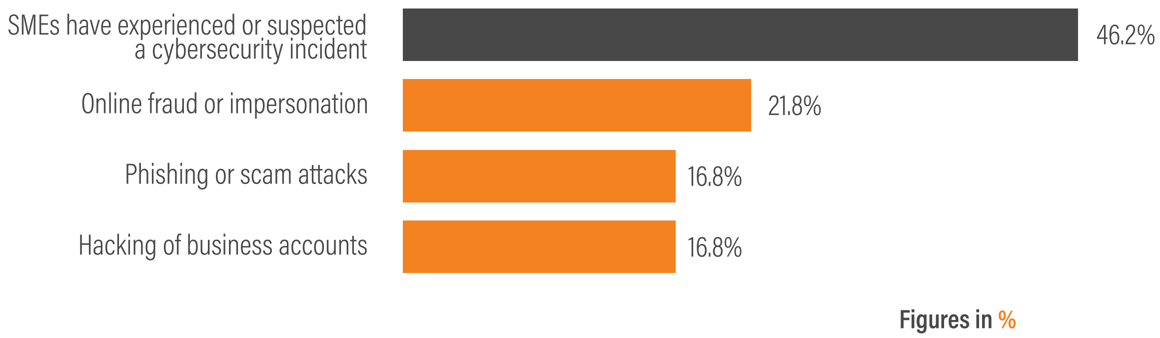
#### c) Hacking of Business Accounts

Unauthorized access to:

- Social media accounts
- Email systems
- Financial platforms

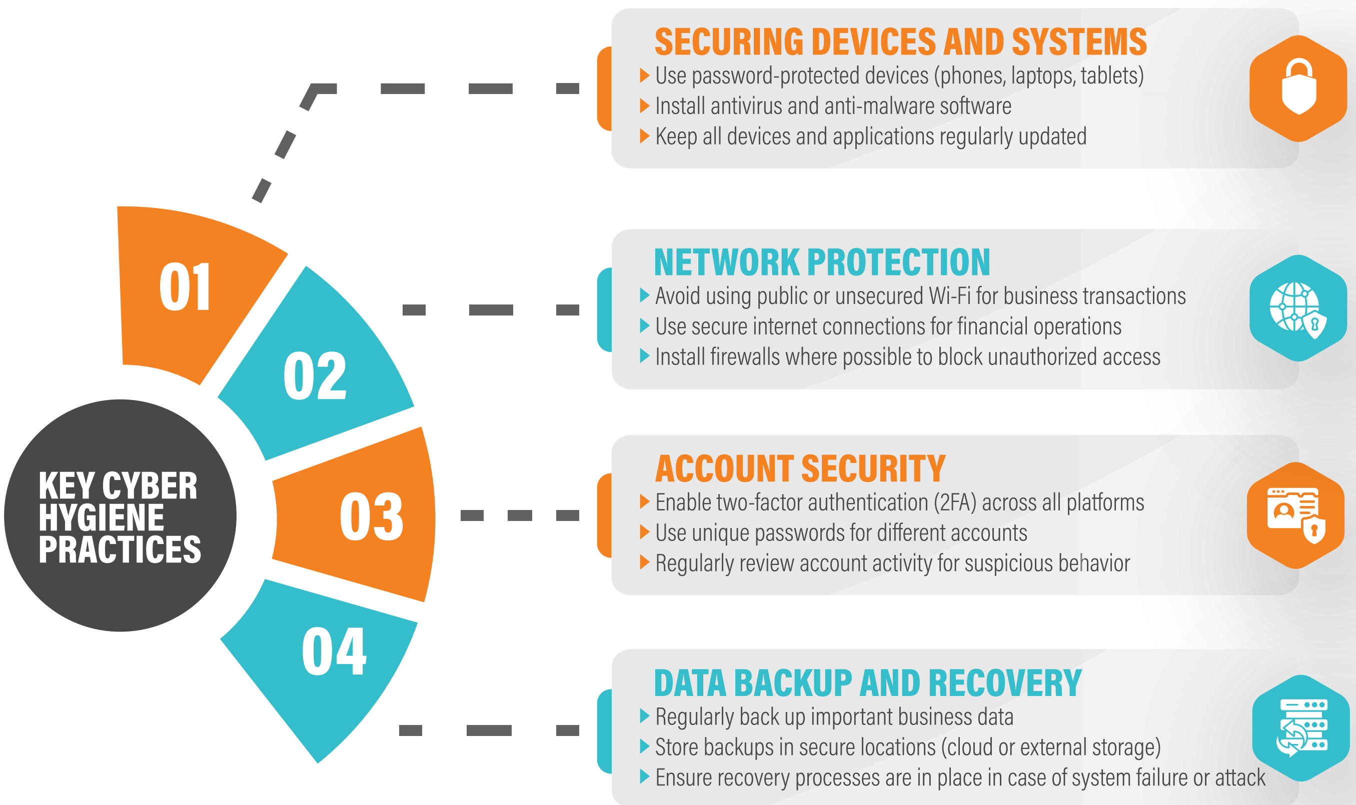
This can lead to loss of control over business pages, Financial theft and Reputational damage

## REALITY FROM THE DATA




### Basic Cyber Hygiene Practices

Cyber hygiene refers to the routine practices and actions that businesses take to maintain the security and integrity of their systems and data. These are foundational steps that significantly reduce exposure to cyber threats.



## EMPLOYEE TRAINING AND AWARENESS

Human error remains one of the leading causes of cybersecurity breaches. Employees who are unaware of risks can unintentionally expose businesses to attacks.

### Importance of Staff Training

Training employees helps them:

- Recognize phishing attempts and suspicious links
- Understand proper data handling procedures
- Avoid unsafe practices such as sharing passwords
- Respond appropriately to potential threats

### Key Areas for Staff Training

- Identifying fraudulent messages and scams
- Safe use of social media and communication tools
- Password management and account security
- Reporting suspicious activity

**24.4%**

Of SMEs train staff on data protection

This highlights a critical capacity gap, where businesses rely on digital tools but lack the human skills to use the securely.

## EMERGING CYBER THREATS

As SMEs continue to digitize, cyber threats are becoming more targeted, sophisticated, and frequent.

### Key Trends Affecting SMEs

- Increased targeting of social media-based businesses
- Growth in mobile money fraud schemes
- More advanced phishing techniques that mimic legitimate services
- Rising cases of account takeovers and identity theft

### Why SMEs Are Vulnerable

- Limited technical expertise
- Low adoption of security measures
- High reliance on digital platforms without safeguards
- Perception that small businesses are less likely to be targeted

In reality, SMEs are often primary targets because they are easier to exploit.

**46.2%**

Of SMEs have experienced or suspected cyber incidents

## Developing a Security Culture

Cybersecurity is not just a technical issue, it is a business culture issue. SMEs must embed security awareness into their daily operations.

### What a Security Culture Looks Like

- Staff are aware of risks and trained regularly
- Security practices are part of daily routines
- Data protection is treated as a business priority
- Management actively promotes responsible data handling

### Practical Steps to Build a Security Culture

- Conduct regular training sessions
- Establish clear data handling policies
- Encourage staff to report suspicious activity
- Lead by example at management level

**Many businesses lack basic cybersecurity practices**

**These indicators demonstrate a high-risk environment where threats are frequent but preparedness is low.**

# 6 THE ROLE OF DATA CONTROLLERS AND PROCESSORS

# THE ROLE OF DATA CONTROLLERS AND PROCESSORS

## UNDERSTANDING THESE ROLES IS ESSENTIAL FOR COMPLIANCE:

| DATA CONTROLLER (SMES) | DATA PROCESSOR |
|---|---|
| ▸ Determines what data is collected and why<br>▸ Responsible for ensuring data protection and compliance<br>▸ Accountable for how data is handled<br>**Most SMEs fall into this category** | Processes data on behalf of the controller<br>Includes:<br>▸ Payment platforms(MTN MoMo, Flutterwave)<br>▸ Cloud storage services (AWS, Google Cloud)<br>▸ Third-party service providers (Glovo, Uber) |

### SME RESPONSIBILITY

Even when using third parties, SMEs must:

- Ensure partners follow data protection standards
- Avoid sharing data without proper safeguards
- Maintain overall accountability

### Key Indicators and Insights

- A significant proportion of SMEs have low awareness of data protection laws
- Very few have implemented formal compliance structures
- Most operate without clear policies or regulatory alignment

This highlights a systemic gap between:

- Digital adoption, and
- Regulatory compliance readiness

# 7 BUILDING DIGITAL TRUST AND CUSTOMER ENGAGEMENT


# BUILDING DIGITAL TRUST AND CUSTOMER ENGAGEMENT

## TRANSPARENCY AND CUSTOMER TRUST

In a digital business environment, trust is a critical asset. Customers are more likely to engage with, transact with, and remain loyal to businesses that demonstrate transparency and accountability in how they handle personal data.

**Transparency involves clearly communicating:**

- What data is collected
- Why it is collected
- How it is used and stored
- Whether it is shared with third parties

**When businesses are open about their data practices, they:**

- Build customer confidence
- Reduce concerns about misuse of data
- Strengthen long-term relationships

### Why Transparency Matters for SMEs

- SMEs often rely on repeat customers and referrals
- Trust directly impacts customer retention and growth
- Lack of transparency can lead to customer distrust and disengagement

In a competitive digital market, **trust** becomes a differentiator

## CUSTOMER RIGHTS UNDER THE DPPA

The Data Protection and Privacy Act (DPPA), 2019 grants individuals specific rights over their personal data. SMEs must understand and respect these rights to remain compliant and build trust.

### Key Customer Rights

**a) Right to Access**

Customers have the right to:

- Request information about the data a business holds about them
- Understand how their data is being used

**b) Right to Correction**

Customers can request:

- Correction of inaccurate or outdated information
- Updates to their personal details

**c) Right to Deletion**

Customers may request:

- Removal or deletion of their personal data
- Especially where the data is no longer necessary

**d) Right to Consent and Withdrawal**

- Customers must give informed consent before data is collected
- They also have the right to withdraw consent at any time

### Implication for SMEs

Businesses must:

- Be prepared to respond to customer requests
- Maintain organized and accessible records
- Ensure processes exist to update or delete data when required

## HANDLING CUSTOMER COMPLAINTS AND CONCERNS

As digital interactions increase, so does the likelihood of customer concerns related to data use, privacy, or security. SMEs must establish clear mechanisms to handle these concerns effectively.

### BEST PRACTICES FOR HANDLING COMPLAINTS


### WHY THIS MATTERS

Poor handling of complaints can escalate into legal issues or reputational damage.

Effective response builds customer confidence and credibility

## CURRENT GAP

**Many SMEs do not have:**
- Structured complaint handling systems
- Clear processes for addressing data-related concerns

**This creates a risk of unresolved issues and customer dissatisfaction**

## IMPORTANCE OF CLEAR COMMUNICATION

Clear and consistent communication is essential in building **digital trust.**

### What Clear Communication Looks Like
- Simple explanations of data practices
- Easy-to-understand privacy policies
- Transparent updates in case of incidents

### Benefits
- Reduces misunderstandings
- Strengthens customer relationships
- Enhances brand reputation

### Customer-Centric Data Policies

SMEs should design data policies that prioritize customer rights and protection.

### Key Principles
- Collect only necessary data
- Respect customer consent
- Protect data at all times
- Be transparent and accountable

### Strategic Advantage

Businesses that prioritize customer data protection:
- Gain competitive advantage
- Build stronger brand loyalty
- Position themselves as trusted service providers

## KEY DATA PROTECTION GAPS AND INSIGHTS

**Limited No.**
of SMEs have structured complaint handling systems

**A Few**
businesses provide customers with access to their data upon request

**Many SMEs**
lack formal customer-centric data policies

This highlights an opportunity for SMEs to improve **trust, transparency, and engagement**

## KEY TAKE AWAY: DIGITAL TRUST IS BUILT THROUGH;

**Transparency**

**Respect for customer rights**

**Responsive Communication**

SMEs that prioritize these elements can strengthen customer relationships and operate more **confidently in the digital economy.**

# 8 RESOURCE DIRECTORY AND TOOLS FOR SMES

# RESOURCE DIRECTORY AND TOOLS FOR SMES

## Free and Low-Cost Security Tools

To support SMEs in improving their digital security, a range of affordable and accessible tools are available.

### DEVICE AND SYSTEM SECURITY

- Antivirus software (e.g., free antivirus solutions)
- Anti-malware protection tools

### PASSWORD & ACCESS MANAGEMENT

- Password managers
- Two-factor authentication tools


### DATA PROTECTION AND STORAGE

- Secure cloud storage platforms
- Encryption tools for sensitive data

### NETWORK PROTECTION

- Firewall tools
- Secure browsing solutions

### Why These Tools Matter

- They provide basic protection against common threats
- Many are free or low-cost, making them accessible to SMEs.

## POLICY TEMPLATES AND LEGAL RESOURCES

SMEs often lack the expertise to develop formal policies. Providing templates simplifies compliance.

### Recommended Templates

- Privacy policy template
- Data consent form
- Data processing agreement

### Purpose

- Ensure compliance with data protection laws
- Provide clarity and structure in data handling practices

### Training and Support Resources

Capacity building is a key need identified in the data.

### Types of Support

- Digital rights and cybersecurity training programs
- Workshops and awareness sessions
- Mentorship and advisory support

**66.4%**

Of SMEs identified training and capacity building as their top need

This highlights strong demand for knowledge and skills development

## PRACTICAL RESOURCES FOR SMES

### The factbook aims to provide:

- Simple, actionable tools
- Step-by-step guidance
- Easily accessible resources

### These resources enable SMEs to:

- Improve data protection practices
- Enhance cybersecurity readiness
- Achieve compliance more easily

## BUILDING A NETWORK OF SUPPORT

### SMEs are encouraged to:

- Engage with industry organizations
- Participate in training programs
- Collaborate with technology and policy partners

### Benefits

- Access to expertise and shared knowledge
- Improved business resilience
- Opportunities for growth and partnerships

## KEY INDICATORS AND INSIGHTS

| | | |
|---|---|---|
| Low usage of structured digital rights resources among SMEs | Limited access to training and support programs | Strong demand for capacity building initiatives |

CIPESA

**A:** Plot 10B Katalima Crescent Naguru.
P.O.Box 122311, Kampala (U)

**E:** media@cipesa.org

**P:** +256 414 289 502