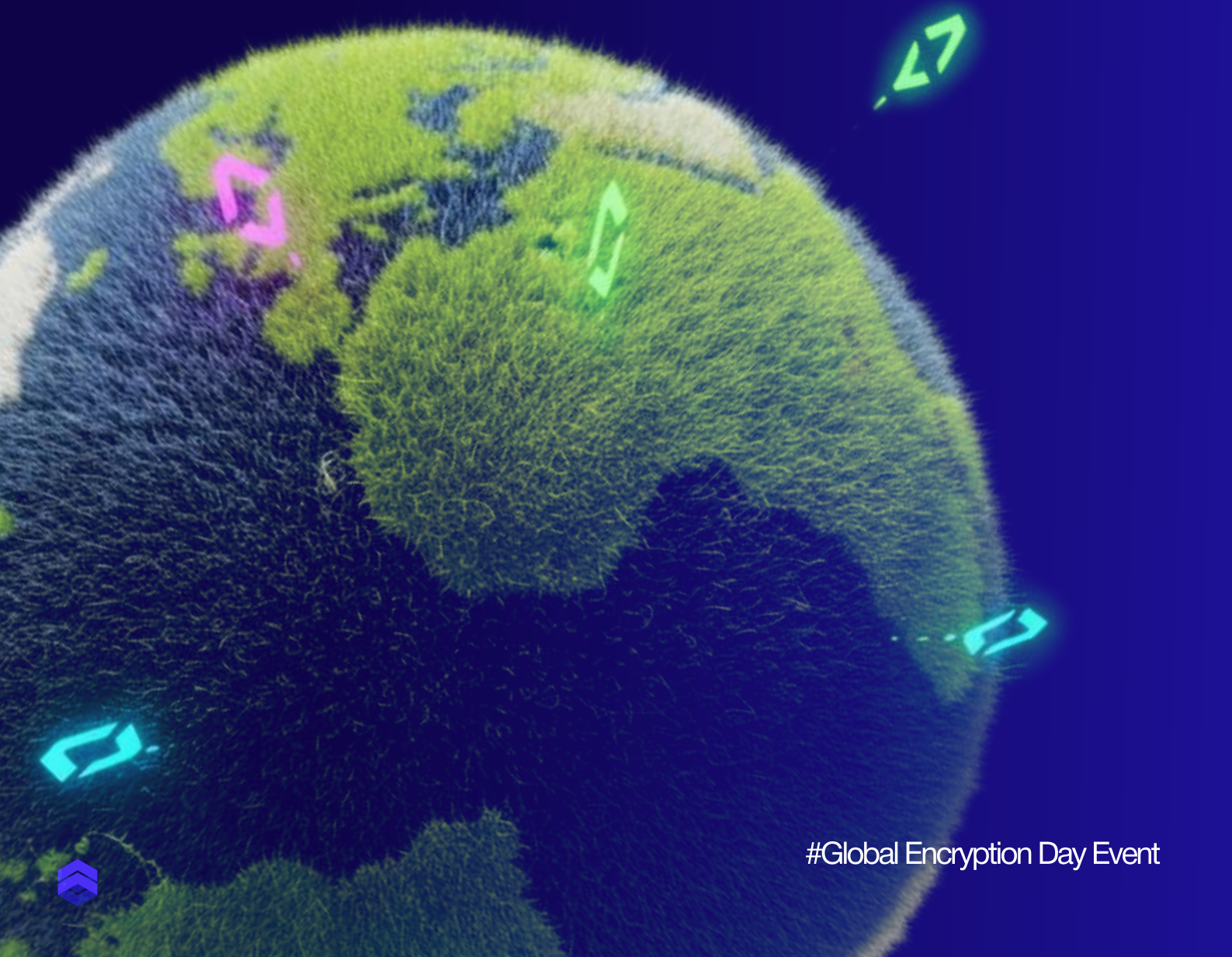
TrustedTech Africa Ltd | Internet Society Foundation

ENCRYPTED BY DESIGN

A Mini-Toolkit for African Tech Startups



#Global Encryption Day Event

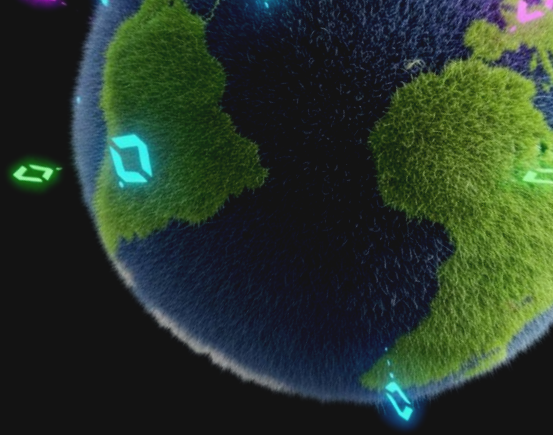


Table of Content

TrustedTech
Africa Ltd

Global Encryption Day Event

Encrypted by Design: A Mini-Toolkit for African Tech Startups

1. Encryption Basics

What is End-to-End Encryption (E2EE)?

End-to-end encryption means data (a message, a file, a note) is scrambled on the sender's device and can only be unscrambled (decrypted) on the intended recipient's device. Nobody in the middle including your servers, cloud provider, or an attacker who breaks into your database can read the contents because they do not hold the secret keys needed to decrypt it. This is different from "encryption in transit" (TLS/HTTPS), which protects data while moving between client and server but still allows a server with the keys to read the data.

End-to-end encryption (E2EE) is like sealing a letter inside a locked envelope where only the sender and the receiver have the key.
No one else, not your internet provider, not the app owner, not even a hacker sitting on the network can open it.

When a platform uses E2EE:

- Data is scrambled on the user's device before it leaves.
- It travels across the internet in a form that looks scrambled.
- Only the intended recipient's device can unlock and read it.

This is especially important when your platform deals with sensitive data such as but not limited to:

- Health information (medical status, medical notes)
- Education records (grades, personal student details)
- Civic engagement data (activism, voting, personal opinions)
- Mental health conversations (therapy notes, crisis chats)

For African founders, E2EE is not a luxury, it's a trust-building feature. It shows users you respect their privacy and helps you stand out in a market where digital trust is often low

How does E2EE work in African contexts?

African tech ecosystems face unique challenges and E2EE can help address them:

- **Low trust in digital platforms** → Many users hesitate to share sensitive information online. E2EE builds credibility by proving their data is private.

- **Shared devices** → In many communities, phones are shared among family or friends. E2EE combined with features like PIN locks and auto-timeouts helps protect private chats and records.

- **Unstable internet & low bandwidth** → E2EE can still work well even in low-connectivity settings, especially when paired with lightweight protocols that don't use much data.

- **Surveillance concerns** → Some users worry about governments or organizations monitoring them. With E2EE, even if data is intercepted, it remains unreadable.

Learn more here: *: How End to End Encryption Works,*

EFF Surveillance Self-Defense Guides

Common Myths About Encryption (Debunked)

Myth 1: Encryption is only for criminals.
🚫 Wrong. Encryption is for everyone. Just like you lock your house even though you're not a thief, you lock your data because it's valuable.

Myth 2: E2EE is too complicated for startups.
🚫 Not true. Open-source tools and libraries (like Signal Protocol or Libsodium) make it easier than ever. You don't have to reinvent the wheel.

Myth 3: Encryption makes platforms slow.
🚫 In reality, modern encryption is lightweight. With good coding practices, users won't even notice it's there.

Myth 4: Users don't care about privacy.
🚫 They do, especially when it comes to health, education, and civic issues. In fact, a strong privacy promise can be a competitive advantage for your startup.

2. Use Cases for Startups

Encrypted-by-Design in Action: Use Cases for Startups

Encryption is not just a technical upgrade, it is a design choice that signals respect for users' dignity, privacy, and safety. Across Africa, startups are already showing how encryption can be woven into products from the ground up, creating safer digital spaces where users feel protected and empowered. In this section, we highlight case studies from African innovators who have applied encryption in practical, context-specific ways from securing therapy notes in mental health apps, to protecting student reports in EdTech platforms, to safeguarding financial transactions in FinTech services. These examples demonstrate that safety-by-design is not theoretical: it is achievable, affordable, and directly linked to user trust and long-term growth.

By learning from these pioneers, founders and developers can see how encryption is more than compliance; it is a competitive advantage and a core part of building trusted technology in Africa.

Case 1: PressPayNg App — Encryption as the Backbone of Education Financing

PressPayNg is a Nigerian education banking and financing app founded by Abiola Metilelu. The startup offers education savings, education loans, school fees crowdfunding through public donations, free soft skill training, scholarships, holiday jobs, education insurance, and health maintenance for students in tertiary institutions. This silver-bullet solution is designed to flatten the curve of education dropout and out-of-school rates in Nigeria, increase enrolment across all levels of education, boost institutional revenue, address infrastructural deficits, and ultimately advance the human capital development index in the country.

Encryption is at the core of PressPayNg' s platform. The company employs industry-standard end-to-end encryption (E2EE) and TLS protocols to secure user communications and financial transactions. Sensitive data such as student records, financial information, and personally identifiable information are encrypted both at rest and in transit. Additionally, tokenization is integrated for payment details, ensuring no raw card or banking data is stored within the system.
The impact has been significant. By implementing encryption and privacy-preserving measures, PressPayNg has built trust with students, parents, and partner institutions who rely on the platform for secure access to education financing. This trust has translated into higher adoption rates, improved retention, and stronger partnerships with financial institutions and regulators critical in a sector as sensitive as education.

Case 2: Kamel — Securing Online Commerce for African Retail Entrepreneurs

Kamel is a social commerce startup that builds essential infrastructure to empower over 100 million retail entrepreneurs across Africa. The platform provides the tools needed for anyone to start, manage, and grow a retail business of any size without access to capital. Its mission is to make commerce accessible to everyone interested in earning online, from vendors and brands seeking to increase sales, to resellers with no products looking to earn from commissions. Today, Kamel powers hundreds of businesses across Nigeria and is trusted by entrepreneurs at various stages of growth.

While Kamel currently relies on the basic encryption provided by HTTPS to secure transactions, this measure has been critical in establishing user confidence. For an online store, HTTPS is the minimum safeguard: without it, customers would not feel safe entering card details or making purchases. Encryption, even at this foundational level, has therefore been central to ensuring that resellers, vendors, and end customers perceive Kamel as a trustworthy marketplace.

The lesson from Kamel's experience is clear: in digital commerce, user trust begins with security. Even small startups can benefit significantly from adopting basic encryption protocols early, as they provide the foundation for scaling toward more advanced privacy and security features in the future.

Case 3: HireGen-AI — Encrypted by Design for Recruitment Data

HireGen-AI is a B2B SaaS platform that uses artificial intelligence to automate hiring workflows for companies across Africa. In the recruitment and HR sector, platforms often manage highly sensitive data: CVs, personal identifiers, interview notes, and hiring strategies. Traditionally, many early HR tech solutions relied on centralized databases with only basic password protection and SSL certificates. This left valuable candidate and employer information vulnerable to leaks or unauthorized access.

From day one, HireGen-AI chose a different path building its platform with encryption at the core. All candidate data, recruiter prompts, and hiring decisions are secured with end-to-end encryption: TLS 1.3 in transit and AES-256 at rest. The platform also implements row-level security and fine-grained access controls, ensuring that even internal system processes can only access authorized data. Looking ahead, HireGen-AI is testing privacy-preserving AI workflows that process recruitment data without ever leaving its secure environment.

This encryption-first design has become a competitive edge. When pitching to enterprise clients, data security and compliance are always top concerns. HireGen-AI's encrypted-by-design architecture builds immediate trust, shortens sales cycles, and reassures clients that their most sensitive hiring data is protected. Early adopters consistently cite security and privacy as key reasons for choosing HireGen-AI over competitors demonstrating how encryption can directly drive growth in a trust-dependent sector like HR tech.

Case 4: Chayil SecureX

Chayil SecureX is a Ghana-based cybersecurity and compliance company focused on empowering small and medium-sized enterprises (SMEs) to secure their operations and meet global data protection standards. The startup provides a suite of services including advisory support, compliance readiness, and implementation of security solutions tailored to SMEs that often lack dedicated security teams.

Encryption is at the core of their platform and services. They integrate data-at-rest encryption to protect client records, guide SMEs in deploying end-to-end encryption (E2EE) across their workflows, and adopt standards aligned with ISO 27001, GDPR, and Ghana's Data Protection Act (Act 843). This multi-layered approach ensures that sensitive data remains private, protected, and compliant with both local and international regulations.

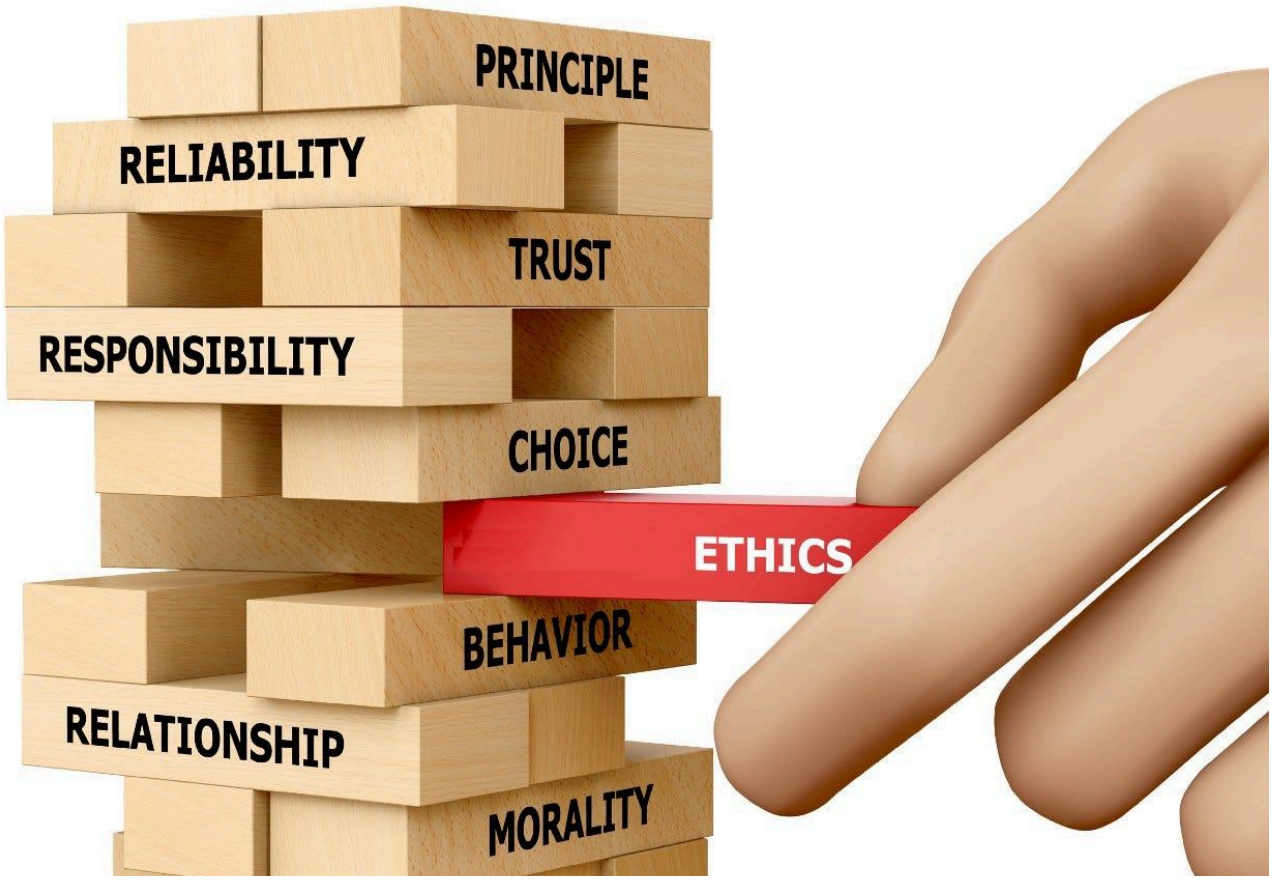
Implementing encryption as a default has helped their SME clients build trust with their customers, confidently meet compliance requirements, and reduce risks of data breaches. For Chayil SecureX, this trust has translated into stronger client retention, new partnerships, and a clear differentiation in the African cybersecurity market as a compliance-first, encryption-first firm

Case 5: Alle-AI

Alle-AI is a multi-modal artificial intelligence platform that enables text, image, audio, and video generation for users across Africa and beyond. The platform is designed to democratize access to advanced AI tools while ensuring that privacy and security remain at the center of its operations.

Encryption plays a vital role in safeguarding the Alle-AI ecosystem. They use secure encryption and hashing techniques for user authentication, ensuring passwords are never stored in plain text. API keys used for connecting with external models and services are encrypted and securely managed. Additionally, sensitive application data including communications and access tokens is encrypted both at rest and in transit, protecting users and preventing unauthorized access.

Their encryption-first approach has strengthened user trust, giving individuals and businesses the confidence that their accounts and data are protected. It has also enabled us to meet the security requirements of enterprise partners, a critical factor in adoption and scaling. By reducing security risks and positioning ourselves as a responsible, privacy-conscious AI platform, Alle-AI has been able to expand its footprint in both African and global markets.



3. Tools & Resources

This section gives you practical, easy ways to start encrypting your platform and protecting user data.

Tutorials & Quick Start

Step 1: Start with the Checklist

We created a simple End-to-End Encryption (E2EE) Checklist just for African startups.

- It helps you figure out where you stand and what actions to take.
- The checklist has drop-downs (Yes / No / To Do) and shows you recommendations automatically.

Download End-to-End Encryption Checklist

Step 2: Pick the Right Tool

Here are some open-source encryption tools, with one video + one guide each.

Need	Tool	Quick Video	Easy Guide	What to Tell Your Developer
Secure messages /chats	Signal Protocol	*How Signal encryption works*	*Libsignal GitHub*	"Please use Signal Protocol for private messaging."
Protect user data in apps	Libsodium	*Libsodium in action*	*QuickStart*	"Use Libsodium to encrypt sensitive app data."
Lock down files & backups	age	*Encrypting and decrypting files at rest using AGE*	*age homepage*	"Encrypt all backups with age."
Secure websites & APIs	OpenSSL + HTTPS	*Getting Started with OpenSSL*	*OpenSSL.org*	"Make sure everything runs over HTTPS."
Encrypt emails & browser apps	OpenPGP.js & PGP with Kleopatra	*How To Use PGP Encryption*	*OpenPGP.js GitHub*	"For browser-based encryption or secure email/file sharing, integrate OpenPGP.js so encryption happens directly in the browser."
Secure cloud files	Cryptomator	*Encrypt Your Cloud Data with Cryptomator*	*Cryptomator*	"Let's use Cryptomator to encrypt sensitive files before uploading them to Google Drive, Dropbox, or OneDrive."

4. UX and Ethics

Encrypted-by-Design in Action: Use Cases for Startups

Encryption is not just a technical upgrade, it is a design choice that signals respect for users' dignity, privacy, and safety. Across Africa, startups are already showing how encryption can be woven into products from the ground up, creating safer digital spaces where users feel protected and empowered. In this section, we highlight case studies from African innovators who have applied encryption in practical, context-specific ways from securing therapy notes in mental health apps, to protecting student reports in EdTech platforms, to safeguarding financial transactions in FinTech services. These examples demonstrate that safety-by-design is not theoretical: it is achievable, affordable, and directly linked to user trust and long-term growth.

By learning from these pioneers, founders and developers can see how encryption is more than compliance; it is a competitive advantage and a core part of building trusted technology in Africa.

Why Ethical UX Design Matters

Every design decision carries ethical weight. The way a button is placed, the default settings chosen, or the notifications pushed to a user all influence behavior. If these choices prioritize business objectives at the expense of user safety, they can create harm.

Ethical UX design matters because it directly affects trust. Encryption is only as powerful as the design that delivers it. If users cannot easily understand whether their communication is private, or if they are nudged into unsafe behaviors, then the promise of encryption collapses. Ethical design makes encryption usable by default and understandable by all, especially those most at risk who may not be tech-savvy.

Why Ethical UX Design Matters

- Clarity and Transparency – Users should know when and how their data is encrypted. Ethical UX design avoids hiding crucial privacy information in fine print.

- Safe by Default – Safe and secure choices should be the default settings. For example, encrypted chats should not require extra steps to activate.

- Accessibility – Privacy and safety tools must be usable by people with varying literacy levels, abilities, and cultural contexts. Complex encryption settings that alienate users are, by design, unethical.

- Respect for Autonomy – Give users real choices. Ethical design avoids dark patterns that manipulate people into oversharing or disabling encryption.

- Protection of Vulnerable Groups – Survivors of gender-based violence, children, activists, and marginalized communities often face the gravest risks. Encryption, paired with ethical design, ensures these groups are not left exposed. Ethical user design asks: Whose safety are we prioritizing? Encryption ensures these groups can communicate, transact, or report abuse without surveillance or retaliation.

Ethical Dilemmas in Startup Design

For startups, the tension between growth and ethics is especially sharp. Founders are under pressure to scale quickly, attract users, and satisfy investors. In that race, it can be tempting to treat UX and safety as afterthoughts.

Some common dilemmas include:

- **Growth vs. Privacy:** Should we prioritize rapid user acquisition by collecting more data or limit data collection to protect users, even if it slows growth?

- **Usability vs. Security:** Should we simplify sign-up by skipping multi-factor authentication, knowing it makes users less safe?

- **Monetization vs. Trust:** Should we design features that nudge users toward oversharing or risky engagement, in the name of advertising revenue?

- **Speed vs. Protection:** Should we ship a new feature quickly to beat competitors, even if its encryption protocols haven't been stress-tested.

In conclusion, Ethical UX provides responsible guidance, while encryption serves as the protective mechanism, and together they ensure user safety and trust in digital platforms.

5. Policy Awareness

Overview of African Data Protection Laws

As a startup, it is crucial to understand and comply with the evolving data protection landscape in Africa. Many African nations have been establishing and strengthening their data protection laws, often drawing inspiration from the EU's General Data Protection Regulation (GDPR). This overview will highlight key features and common principles to help you design a compliant toolkit.

Foundational Principles

Most African data protection laws share core principles that are essential for an "encrypted-by-design" approach:

- Lawfulness, Fairness, and Transparency: Personal data must be processed lawfully, fairly, and transparently.
- Purpose Limitation: Data should be collected for specific, explicit, and legitimate purposes and not be processed further in a way that is incompatible with those purposes.
- Data Minimization: You should only collect personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it was collected.
- Storage Limitation: Data should not be kept longer than is necessary to fulfill the purpose for which it was collected.
- Accuracy: Data must be accurate and kept up to date where necessary.
- Integrity and Confidentiality: You must implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage. This is where "encrypted-by-design" is directly applicable.

The Role of Encryption in Data Protection Across Key African Countries

- Nigeria: Based on the Nigeria Data Protection Act, 2023, encryption is mentioned as a key measure for ensuring data security. The document states in Part VII, Section 39 that data controllers and processors are required to implement "appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data". It explicitly lists "encryption of personal data" as one of the possible measures to achieve this. Additionally, in Section 40 (7), the Act notes that when assessing a personal data breach, the effectiveness of measures taken to mitigate harm such as "any encryption or de-identification of the data" can be considered by both the data controller and the Commission.

- Ghana: Based on the Ghana Data Protection Act, 2012, there is no explicit mention of the term "encryption." The Act does, however, address the broader concept of data security. Section 28 mandates that data controllers take "appropriate, reasonable, technical and organizational measures" to prevent the loss, damage, or unauthorized destruction of personal data. These measures should be regularly verified and updated to address new risks. Similarly, Section 30 requires that data processors comply with the security measures specified in the Act, and that their processing of personal data for a data controller must be governed by a written contract that ensures confidentiality and security.

• South Africa: Based on the South African Protection of Personal Information Act (POPIA), 2013, encryption is not explicitly mentioned by name as a requirement. However, the Act strongly implies its necessity under the broader "Security safeguards" condition. Part A, Condition 7 of the document, specifically Section 19, mandates that a responsible party must take "appropriate, reasonable technical and organizational measures" to secure the integrity and confidentiality of personal information. This is to prevent "loss of, damage to or unauthorized destruction of personal information" and "unlawful access to or processing of personal information. While the term "encryption" is not present, the security measures required by the Act are directly addressed and supported by encryption, making it a critical tool for compliance.

• Kenya: The Kenya Data Protection Act, 2019, explicitly defines "encryption" as the process of converting readable data into a coded form using technical means. The Act requires data controllers and processors to implement appropriate technical and organizational measures to ensure data protection. The law specifically mentions "the pseudonymization and encryption of personal data" as a measure to consider for this purpose. In the event of a personal data breach, communication to the data subject is not required if the data controller has implemented appropriate security safeguards, such as the encryption of the affected personal data.

Documenting Encryption Choices for Funders or Regulators

Key Components of an Encryption Documentation Report

1. Data Classification and Risk Assessment

• **Identify and Classify Data:** First, you must categorize your data based on its sensitivity (e.g., public, restricted, confidential, secret) and the specific regulations that apply to it. Data containing personally identifiable information (PII), financial records, or protected health information (PHI) should be identified as requiring encryption.

• **Assess Risks:** Conduct a data protection impact assessment (DPIA) to identify potential internal and external risks to the personal data you process. This assessment helps you document the reasons for your encryption choices and ensures you are only using the minimum amount of data necessary for your purpose.

2. Technical Implementation Details

• **Encryption Algorithms:** Specify the algorithms you've chosen, such as AES-256 for symmetric encryption or RSA for asymmetric encryption. Document why these choices are appropriate for your specific needs, considering factors like the volume of data and the balance between performance and security.

• **Data States:** Explain how encryption is applied to data in different states:

• **Data at Rest:** Describe how stored data (e.g., databases, hard drives) is encrypted. This could involve full disk encryption (FDE) or file-level encryption.

• **Data in Transit:** Detail the use of secure protocols like HTTPS to encrypt data as it is transmitted over a network.

• **Cryptographic Libraries:** State that you use well-established, open-source cryptographic libraries rather than building custom solutions, which can be vulnerable.

3. Policies and Procedures

• Encryption Policy: Have a formal policy that outlines the "how" and "why" of encryption within your organization. This policy should include guidelines on when to use encryption, such as for emails containing sensitive data or for all mobile devices.

• Key Management: This is a critical section. Explain your procedures for the entire lifecycle of an encryption key, including its secure generation, storage, rotation, and destruction. Emphasize that keys are stored separately from the encrypted data.

• Access Control: Document the measures in place to restrict access to both encrypted data and the encryption keys. This should include multi-factor authentication (MFA) and granting access on a "need-to-know" basis.

4. Compliance and Monitoring

• Regulatory Alignment: Clearly state how your encryption strategy aligns with specific data protection regulations that apply to your industry and jurisdiction, such as GDPR, HIPAA, or the Nigeria Data Protection Act.

• Regular Audits: Document your plan for regularly testing and evaluating the effectiveness of your security measures. This demonstrates a commitment to a continually updated and effective security posture.

• Incident Response: Outline your procedures for handling a data breach, including how you would notify the relevant authorities and affected individuals. Note that if encrypted data is breached but the keys are not, you may not need to report the breach because the data remains protected

6. Community & Support

Building with encryption doesn't have to be a solo journey. Around the world, startups, researchers, policymakers, and civil society groups are working together to defend strong encryption and make it easier to adopt. The Global Encryption Coalition (GEC) brings together organizations, companies, and experts who share resources, best practices, and advocacy tools for protecting privacy and security online.

For African startups, tapping into communities like the GEC and other regional networks means access to technical guidance, peer support, and a stronger collective voice in shaping policies that affect encryption. These communities not only provide learning opportunities and practical resources but also amplify the efforts of founders who are embedding safety and privacy into their products from day one.

About TrustedTech Africa

TrustedTech Africa is a leading consultancy dedicated to embedding trust, safety, and accountability into the core of Africa's digital products and platforms. We help startups, accelerators, ecosystem builders, and digital innovators navigate the complex intersections of ethics, safety, law, and public policy, empowering them to grow with integrity and build platforms users can trust.

We partner with digital platforms and support organizations to build resilient, user-first ecosystems that balance innovation with responsibility. Our services include:

- Safety by Design Toolkit Practical, plug-and-play resources to help startups embed trust and safety across their product development lifecycle.

- Capacity Building & Advisory Workshops, manuals, and expert clinics on child safety, ethical AI, content moderation, and digital risk mapping Custom advisory on policy, product, and governance strategies.

- Startup Risk & Readiness Assessment tailored reviews of startup products to identify potential safety risks and regulatory gaps before they scale.
- Trust & Safety Metrics for Ecosystems to help hubs and accelerators institutionalize trust and safety as a success factor integrating it into selection criteria, impact frameworks, and readiness indicators.

To learn more or explore partnership opportunities:

info@trustedtechafrica.com

www.trustedtechafrica.com