TOOLKIT: RESPONSIBLE CASH

Customer data protection

Why data protection matters: Let's hear Amina's story!

"I was grateful for the humanitarian assistance, but now I live in fear. The mobile money agent wrote my personal information on his logbook, but the next client could see everything as he wrote down his data on the same page. He didn't receive assistance though, and now I feel he stares at me with hostility as he saw how much I received. He now knows where I live, and he even got my phone number and sends me harassing messages."

- As Financial Service Provider, you manage highly sensitive personal data about your clients which is required by national regulations to identity customers. Misusing the data causes harm to people. Your staff and agents interact directly with clients, including disadvantaged groups such as migrants, ethnic minorities, persons with disabilities or survivors of gender-based violence (GBV) etc., posing unique risks:

Your clients' safety

Leaking personal data can expose disadvantaged groups to further harm, fraud retaliation, or discrimination.

Your reputation

A non-secure system damages trust with clients and partners, hindering your reputation.

Legal risks

Many countries have strict data protection laws, so do humanitarian actors. Non-compliance can lead to penalties.

Financial losses

Data breaches can disrupt business operations and lead to financial losses.

Protecting client data is good for business!

- In India, 63% of a test group chose a 11% interest-rate loan over a 9% loan to gain higher privacy features. In Kenya, 64% of a test group chose a 10% interest-rate loan with data protection over a 5% loan (CGAP).
- *Remember:* In countries where literacy rates are low, language barriers high, and connections unreliable, customers are unable to give truly informed consent.

Here are **9 tips to protect your client's personal information**:

1 Empower clients

Empower clients to control their own data. Allow them to easily access, correct, erase and restrict their data free of charge.

2 Train client-facing staff

Train client-facing staff and agents to conduct transactions discreetly, ensure that sensitive information is not overheard or exposed, no photos of people are taken without consent etc. Regularly verify agent compliance through monitoring. Conduct simulations to prepare staff for potential data breaches.

3 Review contract clauses (incl. contractors)

Include data protection, confidentiality of personal data in contracts with your staff, agents and other contracted third parties/business partners. Never share personal information without people's clear consent. All decisions must be in your customer's best interest.

4 Boost reporting channels

Establish reporting mechanisms for clients to report misconduct, identity theft, fraud or other abuse (incl anonymous)

5 Minimize data collection

Only collect the essential information needed for service delivery. Seek informed consent before collecting personal data, ensuring individuals understand how their data will be used. Avoid collecting sensitive data unless absolutely necessary.

6 Protect highly sensitive information

Establish strict protocols for handling very sensitive data (Gender-based violence survivors', people living with HIV, LGBTQI+). Provide specialized training for agents and call centers on handling sensitive how to do referrals without causing harm.

7 Strengthen data security

Use coded identifiers instead of directly identifiable data whenever possible. Encrypt stored and transmitted data to prevent unauthorized access. Restrict access to only necessary personnel. Implement strong authentication (e.g., biometrics, PINs) for account security. Store sensitive data securely and delete it when no longer needed.

8 Use secure digital tools

Use secure devices and networks. Where possible, discourage the use of personal mobile devices for work-related activities

Discover new approaches to data privacy and protection here, as well as the EU standards.