DIGITAL SAVINGS GROUP (DSG) TOOLKIT

DATA PRIVACY AND SECURITY

KEY QUESTIONS TO ASK TECHNOLOGY PROVIDERS

Global Communities

WOMEN FOR WOMEN INTERNATIONAL

DSG TOOLKIT:

DATA PRIVACY AND SECURITY

KEY QUESTIONS TO ASK TECHNOLOGY PROVIDERS

Global Communities
Partners for Good

WOMEN FOR WOMEN INTERNATIONAL

Authors

Lauren Hendricks, consultant
Dennis Mello, Global Communities
Paulina (Paula) Rudnicka, Global Communities

Acknowledgments

The authors are grateful for the valuable contributions of multiple people. Iris Navarro (Women for Women International), Mellisa Mazingi (Women for Women International), Theogene Ruhumuriza (Women for Women Rwanda), Philipos Ageze (Global Communities), Hillary Dashina (Global Communities). Special thanks to colleagues from Tanzania (Global Communities), Ethiopia (Global Communities) and Rwanda (Women for Women) for their contributions to the formative gender analyses and peer-review workshops.

Additional thanks to those who provided inputs during the peer-review roundtable discussions: Tamrat Abera (Mercy Corps), marc bavois (CRS), Koen De Beer (Cyclos), Bindi Jhaveri (Grameen Foundation), Tigist Mengitsu (Jamii-One), Yukiko Yamada Morovic (World Vision), Ethel Mulenga (World Vision), David Panetta (LGP), Courtney Purvis (World Relief), Charlotte Ronje (Jamii-One), Karen Vandergaag (CARE), and Wes Wasson (DreamStart Labs).

The Digital Savings Group (DSG) Toolkit was developed by Global Communities in partnership with Women for Women International. Work began under the SEEP Network's Women Saving for Resilience (WS4R) Innovation Fund, funded by the Bill & Melinda Gates Foundation, and was completed through the generous support of other donors.

Organizational Websites

www.globalcommunities.org
www.womenforwomen.org
www.dsghub.org

INTRODUCTION

Recent years have seen an increased interest in, demand for, and introduction of digital tools for savings groups around the globe. There now exists a wide range of digital solutions which allow savings groups to do many things, including digitizing their record keeping, replacing physical cash with digital wallets and mobile money, and more.

The digitization of savings groups has the potential to accelerate the many benefits of traditional savings groups by expanding digital identities and bridging the gap to formal financial services, particularly for women. It may also help facilitate participation in the formal economy. We have to remember, however, that digitization happens in the context of a persistent gender digital divide, where women's access to and use of mobile and digital technologies are constrained by rigid gender norms, unequal power dynamics, and resource limitations. Our research shows that if not done right, digitization can have negative consequences for women's ability to participate in, lead, and benefit from savings groups. Without adequate training and support, women may experience marginalization and exclusion, especially in mixed-gender groups, where men are often more tech-savvy and therefore more likely to play leadership and digital recordkeeping roles. Women may also face increased risks of data privacy violations and gender-based violence, including technology-facilitated violence.

While the number of technology solutions for savings groups continues to grow, there exists little by way of guidance and tools to support implementers, trainers and groups as they progress through the various stages of digitization. To address this, Global Communities and Women for Women International created the **Digital Savings Group (DSG) Toolkit**. The toolkit consists of seven practical tools to support safe, effective, and gender-responsive digitization of savings groups. These tools include practical guidance for implementers and trainers across multiple aspects of digitization. There is a tool to help implementers gauge their preparedness to launch or expand a DSG project (Digital Preparedness Checklist); a Project Staffing tool to explore changes in the positions and skills needed to support a DSG project; a Monitoring and Evaluation tool to identify key evaluation domains and indicators; tips on Promoting Women's Digital Capabilities; a tool on Addressing Risks of Gender-based Violence; a series of Digital User Dialogues for use directly with savings group members; and a Data Privacy and Security tool with key questions implementers should ask technology providers when considering a digital solution.

Each tool was designed so it can be used by those implementers just beginning to think about their first digital savings group project or by those who are mid-project or preparing to expand. They can be used individually or as a complete set, depending upon the needs of the implementer.

DIGITAL SAVINGS GROUP (DSG) TOOKLIT - *Toolkit "Map"*

The DSG Toolkit consists of seven practical tools to support safe, effective, and gender-responsive digitization of savings groups. These tools can be used in any order, individually, or in combination, depending upon the specific needs of each organization.

The DSG Toolkit was developed by Global Communities in partnership with Women for Women International. Work began under the SEEP Network's Women Saving for Resilience (WS4R) Innovation Fund, funded by the Bill & Melinda Gates Foundation, and was completed through the generous support of other donors.

DATA PRIVACY AND SECURITY

KEY QUESTIONS TO ASK TECHNOLOGY PROVIDERS

Purpose	Digital transformation offers invaluable benefits to savings group members and implementers, but it comes with new challenges related to consumer protection. This includes risks of data privacy violations and data security breaches, which can damage members' personal and financial well-being, while also creating serious legal, financial and reputational implications for entities supporting SGs including implementing organizations and their vendors. By design, digital solutions for savings groups collect a wide range of data from DSG members, including their financial records and personally identifiable information (PII), such as names, photographs, phone or national identity numbers. Digital solution providers (e.g., fintech companies) are de-facto custodians of group and member data, which can be prone to hacking, manipulation and cyber-attacks if appropriate protocols for data collection, storage, processing, use, transfer, alternation, disclosure or deletion are not in place. Implementing organizations must understand these risks and data protection measures must be integrated into a digital solution's architecture before introducing it to savings groups. This tool is designed to help DSG implementers ask technology providers the right questions about their data security policies and protocols, with the goal of protecting the data privacy rights of DSG members.
Audience	This tool is intended for staff of organizations implementing DSG projects, specifically program designers, program managers, information technology (IT) managers, data protection specialists and general counsels.
Time needed to implement the tool	• Review of the tool – 30 minutes • Conversations and the collection of information from digital solution providers – time to be determined by project managers • Additional research about local and global data privacy and security standards – time to be determined by project managers, data protection specialists and general counsel
How to use this tool	The tool defines data privacy and security in the context of DSGs and includes a list of questions to ask digital solution providers while evaluating their vendor proposals.

continued on next page

How to use the tool - continued	Implementers can include these questions in their requests for proposals and use them to guide their conversations and contract negotiations with vendors. In either case, implementers should ask vendors to answer these questions in writing. Some issues are complex, and it is important to ask for clarification until satisfactory answers are obtained. Ideally, questions listed in the tool should be addressed in the process of selecting a digital solution for savings groups, before starting implementation. The tool will also be useful for organizations that are already using a digital solution to support savings groups, especially if there are concerns about data privacy and security or if the technology provider plans to introduce new software features which may increase data privacy and security risks. Implementers are also encouraged to use the companion tool, "Digital User Dialogues," to facilitate conversations with DSG members about how their data will be used, secured and what steps they can take as a group or on their own to further protect their data. Implementers and their vendors should review data privacy laws applicable to national markets where DSG solutions are being deployed. They should also consider applying best practices and globally recognized data privacy standards, even if they are not legally bound by them. This includes, for example, the General Data Protection Regulation (GDPR) of the European Union.
References	Digital Savings Groups Learning Brief (2020) Quickly Identifying Potential Data Risks (2022)

Definitions

While data privacy and data security are sometimes used interchangeably, they are different. Data privacy refers to the rights of individuals with respect to their personal information, and the proper usage, collection, retention, deletion and storage of data. Whereas data security refers to policies, methods and means to secure personal data.

Data Privacy

The protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.
(Sources: CloudFlare, Data Privacy Manager)

Data Security

Controls, standard policies and procedures to protect data from a range of issues, including unauthorized access, accidental loss or destruction.
(Sources: Digital Guardian, Data Privacy Manager)

In this tool, data protection (security) is understood as systems and processes designed to secure the privacy, availability and integrity of data collected through mobile phones. This includes prevention of unauthorized access or misuse of data that mobile phone users have agreed to share. Data privacy is defined as the right of mobile phone users to have control over how their personal data, including personally identifiable and financial information, is collected, stored and used.

Data Privacy and Security Questions to Ask Digital Solution Providers

1. *Do you have a Privacy Policy? Is it publicly available? Can you please share it with us?*
2. *Do you have a Data Protection Officer?*
3. *What the data security protocol for your product?*

   Data security protocols are the software and behavioral rules that guide how employees handle and access data collected through websites or mobile applications, such as those used to manage DSGs. These protocols should include strong encryption when transmitting data and storing it on both the mobile phone and server. Vendors should have clear guidelines that demonstrate the organization's approach to data security. This will include things like SSL certificates (digital certificates that authenticate a website or a mobile application's identity and enables an encrypted connection), virtual private networks (VPNs), multi-factor authentication and more.

   Security controls should be publicly available. If a vendor must draft them specifically in response to your request or has trouble explaining them, they may not have adequate controls in place.

4. ***Have you conducted data mapping for your product? If yes, can you please share it with us? If not, please answer the following questions.***

   Conducting data mapping is a crucial first step in ensuring compliance with data privacy laws, standards and best practices. It is imperative to know what data will be collected from DSG members through the digital solution, how this data will be stored and transferred, whether an internal or external party will have access to it and what safeguards are in place to protect this data (e.g., IT controls or contractual protections). Please note that a vendor may ask for a non-disclosure or confidentiality agreement prior to disclosure, which is typical.

   a) What data does your product collect from savings group members? Please include both sensitive and non-sensitive data points, including all personally identifiable information (PII) and location data if applicable.

   b) How will you protect the rights of DSG members as data subjects?
      - Right to information
      - Right of access
      - Right of rectification
      - Right to erasure
      - Right to restrict/object to processing
      - Right of data portability
      - Right to object
      - Right to be notified of data breaches
      - Right to avoid automated decision-making

   c) Where will DSG group and DSG members data be stored?

   Vendors can store data in a variety of places, like on premises, in the cloud or both. Make sure you understand where the DSG data is being stored and how it is backed up.

   Companies with remote employees should be optimized for mobile and virtual platforms, as well as able to provide a consistent and secure environment for them to access data.

   d) How will you process and use DSG member data?

   e) Who will have the capacity to alter, archive or destroy DSG member data?

5. *Have you achieved any recognized data protection standards?*

   There are a variety of data protection standards governing how organizations approach data security: ISO 27001, SSAE16, and Safe Harbor, among others, these provide companies with a clear blueprint dictating how to safeguard data. ISO 27701 is the new international standard in data privacy and is particularly noteworthy. It was designed with the General Data Protection Regulation's (GDPR) principles of privacy by design and by default in mind, so it is fully compliant with modern data protection standards and expectations.

   Your vendor may be too small to be certified by any of these standards, but it is worth asking. Even if they are not certified, it is good to understand if they adhere to certain standards.

6. *How do you assess your employees' knowledge about data security?*

   Some of the most damaging data breaches result from human error. In an ideal world, your vendor will conduct regular data protection training, or it might be part of new employee onboarding.

7. *Do you separate customer data from the main infrastructure?*

   If your vendor's main infrastructure is hacked, you want to know that the DSG members' data is safe — ideally in a cloud-based environment.

   If they are kept separately, it is also worth enquiring about internal access controls. It is important that only necessary users can access client information. Cloud computing can be highly secure if the right access controls are in place and customer data is kept separate from the main infrastructure.

8. *Do you work with other third parties to deliver your solution? Do they have access to DSG member data? If yes, what are their data security protocols?*

   Many vendors rely on third parties for part of their solution, and those vendors might not have tight data security protocols. Using a third-party is not in and of itself concerning; it is quite common for Software as a Service (SaaS) companies. You need to enquire about third-party data protection policies and standards.

9. *What is your disaster recovery plan for your product?*

   No matter how tight their security, there is always the chance that the vendor will suffer a data breach. In that event, they need to have a solid recovery plan in place. Not only will it help protect the DSG member data, but it means they can get back up and running as soon as possible.

10. *Do you perform routine disaster recovery tests for your product?*

    A plan is only as good as its execution. Routine tests prove that security is a top priority, and they make sure that everyone knows what is expected of them in a crisis. Disaster recovery tests ensure the recovery plan is completed as smoothly and painlessly as possible.

11. *Are you GDPR compliant?*

    Depending on your donor requirements, you may need your vendor to be GDPR compliant. GDPR applies to all companies that conduct business or engage with customers in the European Union.

12. *What are my data privacy compliance needs from a legal and ethical standpoint?*

    This is something you should understand before you talk to your vendor. But the vendor should also be able to advise you on these issues in your jurisdiction, and they should understand and ensure that you follow legal standards.

    Increasingly countries have data sovereignty laws that guide how data gathered from citizens can be stored and used. You should seek legal counsel, even if you outsource your data storage and management to a service provider, you likely have legal liability. Be sure to thoroughly check your vendor's track record and credentials to ensure they can handle your unique data compliance and security needs.

13. *What is your software update policy?*

    Old software can put systems and networks at risk for cyberattacks. That is why it is a good idea to ask the vendor if they automatically update their software solutions.

14. *Do you have filters or similar features that will protect DSG members from cyberthreats?*

    Does the solution have built-in protection that stops things like malware and phishing messages from reaching people who use the tool?

15. *Who will have access to DSG member data? Please include all internal and external parties.*

    What DSG member data do you share or plan to share with third parties (i.e., implementing organization or a financial service provider)?

    When selecting a vendor, you want to understand who owns client (DSG member) data. Is it the vendor or the implementing organization? If the vendor owns the data, which may be common for DSG solutions, what rights do you as the implementing partner have to access, process or use that data? Will you have access to raw data or only to reports generated by the solution? Will you have access to individual member data (e.g., names or phone numbers) or only group-level data (groups' savings balances)?

    Before signing a contract, it is important to know whether or how the vendor is entitled to share, sell or otherwise use DSG member data, even if they are the ultimate owner of the data. Your vendor should have a data privacy policy that they can share with you.

16. *How does your product ensure user awareness and consent around data collection, processing and sharing?*

    Many DSG platforms are designed to provide data to third parties in order to improve DSG members' access to financial services. But any vendor you work with should have processes in place to request user consent for any data sharing with third parties that includes personally identifiable data, including name, identification numbers, phone numbers or addresses.

    Ask specifics on the consent request, including a copy of their policy on user consent. A blanket data sharing agreement in an applications' 'Terms and Conditions' should not be considered adequate and is often not in compliance with local and global laws, including GDPR. A consent request needs to be presented in a clear and concise way, using language that is easy to understand and be clearly distinguishable from other pieces of information such as terms and conditions. The request must specify what use will be made of personal data and include the name of the company accessing the data. Consent must be freely given, specific, informed and unambiguous.