Global Fund for Women Digital Protection Guidelines

Digital Security Principles

Global Fund for Women minimally adheres to the following data protection principles. This includes both internal processes and relevant notices for subjects:

(1) **Fair and Lawful Processing:** Personal data should be used in ways the individual would expect. Individuals should be informed about any processing caried out about them. There should be a lawful basis for the processing, for example: consent.

(2) **Purpose Limited Processing**: Personal data should be processed for one or more specific purposes. Individuals should be informed about the purpose for which we are processing their data.

(3) **Retention**: Personal Data should not be kept longer than necessary. Once it has fulfilled its purpose, it should be deleted or anonymized. Individuals should be informed of the retention period.

(4) **Data Subject Rights**: Individuals have numerous rights related to their personal data. Processing should be carried out in accordance to hose rights, for example, the rights of access, rectification, right to opt-out, right to delete. Information should be provided to individuals about how to enforce their rights, and processes but in place to enable this.

(5) **No excessive use**: any personal data use should be adequate, relevant, and not excessive. This means, using enough data for the intended purpose, using the right data for the intended purpose, and only collecting personal data needed to fulfill the purpose and no more.

(6) **Data Security**: Personal data should be kept secure. Security measures should reflect the sensitivity of the data, the data use, and the risk and harm (to individuals) if the data was exposed.

(7) **Data Accuracy**: Personal data should be accurate (correct) and should be kept up to date.

(8) **Data Transfers**: individuals must be informed if their data is leaving the country and where it goes. If data is to be shared with third parties, individuals must be notified that it is being shared and why; the security of the third party must be evaluated; and a data processing agreement should be in place. Data transfers should be secure.

Best Practices

Global Fund for Women receives data on individuals and organizations through self-registration (ex: donations, newsletter sign-ups), solicitation (ex: surveys, research), and transfers (ex: donor lists, referrals). Our goal is to ensure the safeguarding of information including both privacy and security practices, with particular attention to personal and sensitive information, and adherence to data minimization principles. Please review the Privacy Champions Training Session.

1. Before Collecting, Processing or Transferring Data

- Define specified purpose of research, processing, or transfer.
- Consider vulnerable/marginalized populations' right to be heard and included in research, and balance with their right to privacy and security
- Define specific data that will be collected, processed or transferred, identifying private or sensitive information that will be included.
- Consider data sensitivity and carry out risk assessment to ensure unintended consequences will arise as a result of our data collection efforts
- Complete GFW Privacy Review Template
- Review local legislation around data privacy & protection, using DLA PIPER
- When applicable, submit research design protocols and supporting tools to local and US Institutional Review Boards for approval

2. Collecting, Processing or Transferring Data

- Develop research design protocols and supporting tools
- Reference the Fund Compliance Pack for agreements, notices, and security do's and don'ts. Ensure alignment and working links to Global Fund for Women's Privacy Policy
- Create or update informed consent processes in alignment with the fund compliance pack and with reference to safeguarding participant data.
- Complete a Privacy Impact Assessment, for collection, new processing, or transfer, which includes:
    - Defining the collection, maintenance, access, storage, and disposal of data.
    - Assessing transfers and legalities and technicalities for transferring across countries.
    - Security assessments of third-party data providers, evaluating security practices, data protection measures, and compliances with industry standards.
- Prioritize vendors who have been vetted by Global Fund for Women counsel, with up-to-date agreements and notices on processing locations.
- Ensure alignment
    - Box and Qualtrics are vetted vendors.
- If data is collected first-hand by GFW or it's personnel:
    - Obtain informed and voluntary consent from potential participants. Adapt notices provided in the compliance pack.
    - Be transparent about purpose of data collection
    - Collect data for original specified purpose only, or obtain express consent for further use
    - Limit the collection of personal data to "as needed" basis only. Where possible, do not retain

    - Train enumerators on proper process for data collection, capturing and storage
    - Train enumerators/interviewers on using Trauma Informed Approach
    - Share contact information of project manager or lead researcher with participants
    - Establish data protection standards ahead of data collection (see following sections)
- If data is collected by third-party:
    - Establish an agreement utilizing this service agreement template; including terms of data access, usage, and sharing.
    - Provide notices and compliance pack to third-party to evaluate compliance with Global Fund for Women's policies.
    - Conduct security assessments of third-party data providers to evaluate their security practices, data protection measures, and compliance with industry standards. Consider factors such as data encryption, access controls, incident response capabilities, and overall security posture.
    - Ensure the process for individuals to unsubscribe/opt-out is working and correctly reflected in the notices used.
    - When sharing Global Fund for Women contacts with third party, ensure you have consent for this processing (and sharing) and it is screened against any opt-out lists you have in Box or Qualtrics before shared. Share these only through secure transmission method.
    - Consider masking or anonymizing sensitive data elements before accessing or using third-party data, especially if the data contains personally identifiable information (PII) or other sensitive information.
    - Conduct a Privacy Impact Assessment for new surveys.
    - Provide resources to third party on Security Do's and Don'ts.
    - Implement access controls to restrict access to third-party data based on roles and responsibilities. Only authorized GFW individuals should be granted access to the data, and their access should be regularly reviewed and updated as needed.
    - Follow best practices for data integration to ensure the seamless and secure integration of third-party data with systems. Implement validation checks, data cleansing, and error handling mechanisms to maintain data integrity.
    - Monitor access to third-party data for any suspicious or unauthorized activities.
    - User Training and Awareness: Provide training and awareness programs to employees who access third-party data to educate them about data security best practices, privacy considerations, and their roles and responsibilities in safeguarding the data.
- Where possible, design data collection to ensure participants can revoke access automatically. This includes specifying the process for opt-ing out in communications and/or providing a contact for revocation.

3. Managing, Using and Storing Data

Global Fund for Women staff and third parties must adhere to data protection principles, including:

- Use the collected data in consistency with stated specific purpose of the activity. Data collected on grantees, personnel, donors, and any other party will be used in ways that respect their privacy and minimizes risks of harm.

- Subsequent processing of existing data must first review consent and existing Privacy Impact Assessment to ensure new processing does not require a new or updated assessment.
    - If new processing falls outside the existing assessment and consent, must request consent from involved parties.
    - If new processing falls within the existing assessment and consent, must include in produced materials.
- Where possible, anonymize or de-identify personal information; ideally, delink sensitive and personal information to minimize risk.
- Maintain high quality of data (accuracy, up to date, unbiased)
- Train/equip those handling data with information management/protection skills
- Ensure privacy and confidentiality of any personal or sensitive data, including limiting internal, Global Fund for Women access to those with explicit purposes. Consent documentation to be stored alongside data, stories, photos or other digital assets.
- Ensure reasonable physical and technical security safeguards to store data
    - Any devices used for data collection will be password-protected to prevent unauthorized access.
    - Ensuring privacy is the default setting when designing digital applications, services, or platforms.
    - Only GFW authorized devices may be used by staff.
    - Consultants using non Global Fund for Women devices must use password-protections, store files in approved vendor software (ex, Box), and have written guidelines for final transfer of data materials.
    - Hard copies of confidential and sensitive data are disposed of or destroyed in a secure manner
    - Loss of data on (e.g. lost laptops, pen drives, etc.) is immediately reported to the Sr. Director of Integrity + Compliance and the Senior Director, Learning, Evaluation & Analytics and Global Fund for Women's Data Breach processes is implemented
- Include a data retention agreement in consent form and/or communications. Ensure files with raw data have retention dates included.

4. Sharing and Transferring Data

- Data can only be shared if existing consent covers the purpose of sharing and/or consent for sharing is received from participants.
- Share and transfer data in accordance with specified purpose/use. Adhere to data minimization principles to only include relevant information.
- Screen any data shared against opt-out lists.
- Do not share directly linked personal and sensitive data unless absolutely necessary for the purposes of the transfer. Where possible, anonymize data.
- Assess the sharing/transferring locations' security. Utilize encryption, minimally, if sharing by email. Utilize approved vendors (ex, Box) for enhanced security.
- Create a relevant data sharing agreement, including information on data storage, access, management, and retention.
- Ensure core data protection principles and safeguards while transferring data across borders and complying with local laws using DLA PIPER.
- Consult and update relevant Privacy Impact Assessment
- When receiving transferred data, adhere to the agreed upon security practices and ensure retention dates are included.

- When a third-party has collected data to be transferred, ensure all files related to the data are transferred and stored jointly. This includes consent forms, raw data, processed/cleaned data, coding or analysis scripts, reports and/or presentations.

5. Closing the Feedback Loop

- Notices to participants should include links to Global Fund for Women's privacy policy, contacts, and/or other mechanisms to solicit more information, revoke consent, or otherwise opt-out.
- Provide participants with contact information of Project Manager, privacy@globalfundforwomen.org email, and other options (like Speak Up Line) to reach Global Fund for Women for concerns/feedback
- Respond to participants' concerns/questions/feedback within a reasonable specified time
- Clearly state any benefits/remuneration that participants can expect from their participation
- Do not make promises which cannot be met, and do not set false expectations

6. Disposal of Data Once Purpose is Met

- Review and consider length of time to keep data for each project
- Regularly delete sensitive data where retention is not legally required
- Comply with participant's request to withdraw from a project or to have their data deleted
- If data is collected by a consultant, require their deletion of data through a clause in their independent Contractor Agreement. Have the project manager confirm their completion at the end of the project.
- Acquire necessary expertise and practices to effectively destroy data

7. What to Do in Case of Data Breach

- A breach is any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data, whether accidental or deliberate.
- Report to Sr. Director of Integrity + Compliance and the Senior Director, Learning, Evaluation & Analytics of data breaches without delay after becoming aware
- Provide necessary information in a timely manner to investigate a data breach: document what has been reported, and gather as much data as possible including the number of people affected, who they are, potential risk to them, what data may have been compromised, evidence that data was compromised, and if the breach is ongoing.
- Based on what has been reported, assess risks associated with breach and determine severity
- Involve essential personnel/teams to resolve the breach
- Take necessary measures to ensure safety and protection of individuals affected by breach
- Consider back-up mechanisms and security measures to wipe out data remotely
- Led by Sr. Director of Integrity + Compliance, notify affected participants and any third-party partners

Safeguarding Participant Data

Safeguarding Data of Participants:

In cases where Global Fund for Women is collecting data for public purposes (donor stewardship, communications, published research) a higher threshold for informed consent must be reached. The following guides this process:

- Informed consent is always secured prior to the collection of any data from individual participants, communities, or movements ("participant[s]"). The following consent principles must be followed:
  - Informed Consent: Permission granted in full knowledge of the intent of the data collection and any possible consequences
  - Continued/ Ongoing Consent: Both immediately before and after the data collection process the participants would be required to reconfirm their willingness to share the data collected from them. Participants would have the right to revoke consent before, during and after the data collection
  - Retrospective Consent: The participants' consent would be sought if the data collected needs to be repurposed in any other way, other than the initial intended purpose, at any point in time.
- Consent may be obtained through a signature on a consent form, video/audio recorded consent, or digital confirmation of consent.
- Consent for use of images or stories is distinct from other forms of consent (e.g. consent to participate in activities, research).
- Where a participant lacks the capacity to provide informed consent (e.g. due to age, illness or disability) consent must be obtained from a family member or, where one is unavailable, from a senior member of project staff who has responsibility for the participants well-being.
- No data will be used without informed consent and will be destroyed if this is not secured.
- In all circumstances, consent must demonstrate that the participant understands:
  - How their data will be used and for how long, and by whom
  - How their privacy will be upheld
  - That their consent is voluntary, they have the right to decline, and they can withdraw at any stage in the process by informing any Global Fund for Women staff member of their decision.
- Participants are enabled to give their own accounts and personal narratives, rather than have people speak on their behalf.
- Data or images that could be used to identify the participants specific location (such as village or community names, school, parish, etc.) must not be used without their explicit consent.
- Where participants are survivors of violence or human rights violations, no data is shared which could lead to their identification.
- Work product resulting from data collection efforts will clearly stipulate when names and locations have been changed for protection and privacy purposes.
- Consent is provided to Global Fund for Women and not to any individual.