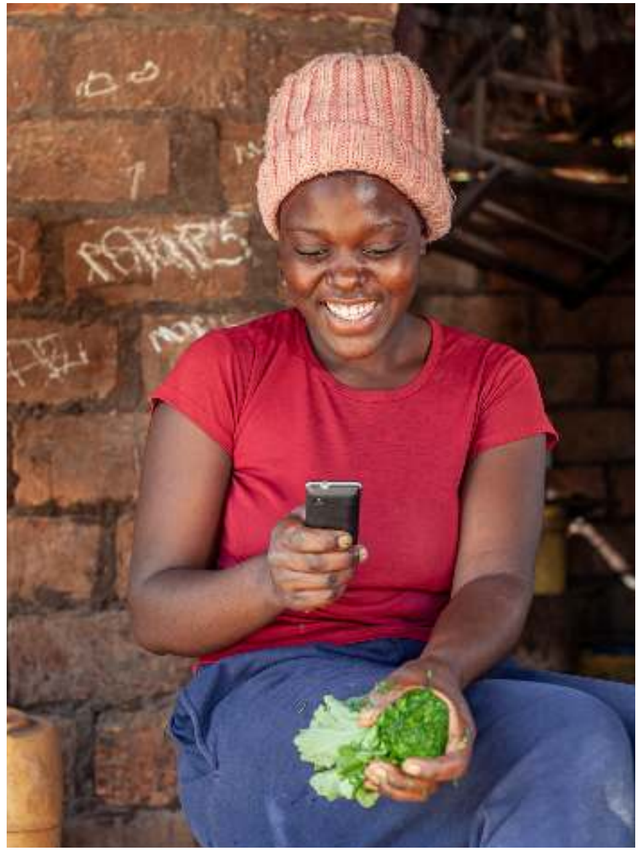
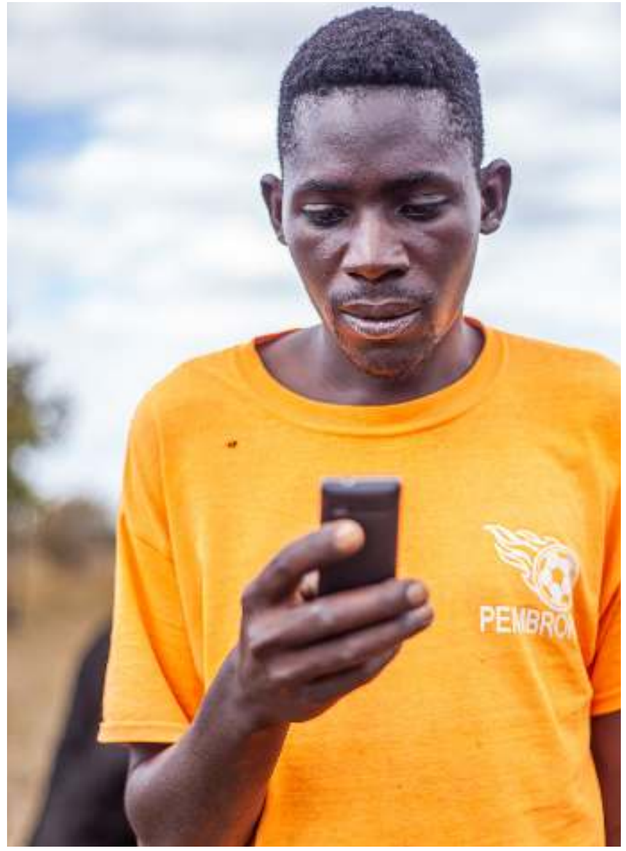
Data and Privacy Processes





Data Protection

Loop is available on many platforms including: SMS, Interactive Voice technology, WhatsApp, Facebook messenger, or via our website.

However, the safest way to share stories is through our website at www.talktoloop.org where we have full control over the data, as opposed to other platforms whose domain isn't within our control.

If a story is marked as sensitive when sharing it through another platform, it will be redirected to Loop, to ensure the data is safe.

Loop takes safety seriously

Our priority is to make sure people can share their opinions and experiences in a safe, open and transparent way, to effect positive social change at individual, community and global level.

The Privacy Policy is designed to keep users safe and protected, enable them to give informed consent and give them confidence that we handle all data sensitively and with the highest security measures available.

Our designers and developers have decades of experience working in Data Security systems across many portfolios: banking, health records, etc

Key Facts

Loop does not collect or process any data unless you share it. Content moderators ensure that nobody else posts information that could identify you.

We will not collect, store, reveal or share your exact location.

We will not share your contact details with anyone, and people can only contact you through the platform. The exception is for stories that may need follow-up or referral to a service, in which case we will always ask you for consent first.

If you change your mind about anything you have chosen to share and want it to be removed, you can contact us and Loop will permanently remove it.

We comply with EU General Data Protection Regulations (GDPR), and apply these globally.

We do all we can to keep your data safe, and the safest way to share sensitive stories is directly through the platform.

What data do we store, and how do we keep it safe?

Any data shared with us is stored on Amazon Web Servers (AWS) in Germany.

Amazon uses Advanced Encryption Standards 256-bit encryption for files both in transit and at rest. We use two-factor authentication.

In January 2022 we had our first annual data security audit, including penetration testing, by an independent specialist and got a glowing result.

We invest in security on an ongoing basis.

How we moderate stories?

To create a safe place to listen and engage, a Loop Moderator reviews all stories or replies and determines whether they are sensitive before they are posted on the open platform.

Based on the Guidelines, Protocols and national risks, the Moderator will either publish the content or reject it. In both cases, if we have the person's contact details, we will let them know.

Three things can happen to each story or reply:
1) A Moderator may remove tags if there is a concern they can be used to identify a person.
2) The Story/ Reply will be rejected and the author informed why, and given an opportunity to re-submit
3) The Story/ Reply will be referred onto a Case Manager and NOT posted on the open platform.

Nothing is posted without going through a trained moderator.

What happens to a Sensitive Story?

A sensitive story will be managed by a specially trained Case Manager and processed through a Case Management tool which only they can access. All Case Managers have signed confidentiality agreements and Codes of Conduct.

Loop Case Managers refer on Sensitive Stories into accepted referral pathways. We do not share any names, contact details or identifiable information with anyone. We will contact the author to inform them of whom we recommend to refer the case on to and ask for their consent to be put in touch for assistance or for further investigation.

It is all based on the Survivor's choice.

Sensitive Story data protection

Information related to a sensitive story is stored in a secure database called Airtable.

Information sent and received by Airtable is encrypted and the data is stored in servers that are certified internationally as highly secure and compliant with 'gold standards'.

Only Loop Case Managers have access to the data using a 2-step verification process. See more details in our Policy.

`

Incorporating best practice and survivor-centred approach

Case Manager SOPs are drafted based on inter-agency best practice guides on GBV, Child Protection and others. All referrals are made using a survivor-centred approach.

The Case Management Tool was designed on the IASC Best Practice Guide on Inter-Agency CBCMs and tracks specific accountability steps.

Security for survivors

Loop does not store any user data on any browser and there is no app to download.

Browser history identifies the story page but no further information.

People using WhatsApp, Facebook messenger, SMS or IVRR may have some data recorded through third party input mechanisms as per all digital tools.

We minimize the number of third parties and we audit their data policies and negotiate better terms where possible.

Loop is complementary and integrated

In each country context, the colleagues on the ground make sure that Loop is integrated into existing referral systems so that survivors can access services as quickly and safely as possible.

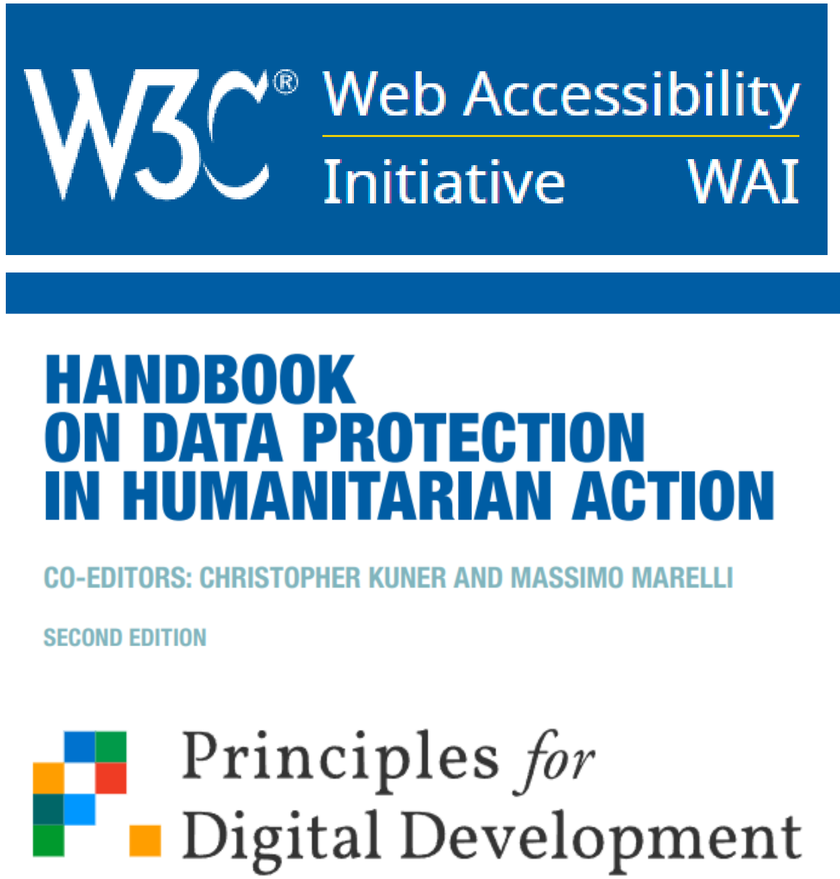
In the Philippines this has meant working with local government authorities and in Zambia with ChildLine/LifeLine and also the One Stop Centres for GBV.

The purpose is to be complementary so that gaps are filled and people protected from harm.

We are aspire to these guidelines

We are constantly learning and improving our tech solutions, training and approaches to ensure a safe environment.

- WCAG 2.1 AA standard. With 11y audits to support improvements
- ICRC - Handbook on Data Protection in Humanitarian Action. 2nd Edition, C. Kuner and Marelli
- GDPR - General Data Protection Regulation or the EU
- Principles for Digital Development



At the interagency level

- Loop can complement and feed into existing inter-agency CBCM
- Loop data can contribute to AAP reporting and indicators
- Loop is an example of a linked AAP and SEA reporting system
- Loop can be implemented by any NGO that does not have existing complaints/ feedback mechanisms thereby strengthening overall AAP and PSEA efforts (e.g. IASC PSEA MOS)
- With enough interest, Loop can be tailored to meet interagency information needs
- Agencies can support national partners to use Loop to increase their AAP/ CEA, SEAH and complaints reporting mechanisms

Interested?

1. Register on Loop so that you are notified if any feedback is about your organisation.
2. Share your reporting pathways with Loop to ensure fast safe referrals to your organisation
3. Promote Loop within your organisation – contact us for help, training, introductions, communications materials, safe guarding questions.
4. Promote Loop within your partner organisations
5. Respond to stories actively
6. Analyse data regularly
7. Include Loop in project proposals, email: alex@talktoloop.org

Queries and Pathway

To get allegations to the right place quickly and confidentially please share your:

- Organisation Name
- Issues to Refer: Sexual Exploitation, Misconduct, Fraud..
- National, Regional, Global levels
- Contact Name/ Name of mechanism
- Role in Organisation
- Email and Phone number
- Countries covered
- Location of person
- Other notes or information

Please also attach any documentation to help us comply with your processes.

Questions?


alex@talktoloop.org


talktoloop.org


@talktoloop


@talktoloop


@ Talk To Loop