



# Data Protection Impact Assessment

Last updated: August 2025

This document details the Loop Data Protection Impact Assessment (DPIA) process and outcome. It follows the process and template set out in the [Information Commissioner's Office's DPIA guidance](#), set out in European guidelines on DPIAs.

## Table of Contents

Part 1: Loop's need for a DPIA	3
Part 2: The Nature of Loop's Processing	4
What is the source of the data?	4
Who do we share data with?	5
Data Collection Minimisation	6
What "Opt In" data do we request & collect?	7
Feedback details	7
Country	7
Location	7
Organisation	7
Author details	8
Name	8
Phone number	8
Email address	9
Data which is tagged:	9
Physical or mental health condition	9
Gender	10
Age	10
Data Download	11
Who is responsible for keeping Loop data safe?	11
What data do we store and how do we keep it safe?	12
Where do we store our data?	12
What data do we share?	14
Information Quality and Accuracy	15
Data Access, Retention & Deletion	16
Part 3: The Consultation Process	16

Stakeholder Groups	16
Community Members and People Affected by Crisis	16
Accessibility	18
Organisations working to help people affected by crisis	18
Donors and others wishing to use the platform's open data in their work and decision making processes - research, policy, advocacy etc	20
Testing of the Loop Systems (Audit)	21
Methodology:	21
Part 4: Assessment of necessity and proportionality	22
Legal basis for data processing and transfer	22
How do we ensure compliance of our Data Processes?	23
Data Subject Rights	24
Consent	24
Part 5: Identify and Assess Risk	27
Source of risk and nature of potential impact on individuals.	27
Likelihood of harm	27
Severity of harm	27
Overall risk	27
1. Authoritarian Governments or others trying to get access to Loop data	27
2. Staff accidental breaches	28
3. Third party breaches	28
Part 6: Measures to reduce risk	29
Risk	29
Options to reduce or eliminate risk	29
Effect on risk	29
Residual risk	29
Measure approved	29
Authoritarian Governments or others trying to get access to Loop data	29
Staff accidental breaches	30
Third Party Breaches	31
Item	32
Name/date	32
Notes	32
<b>Annexes</b>	<b>33</b>
<b>Talk to Loop Compatibility with Somali Law</b>	<b>33</b>
Part 1: What is the Somalia Data Protection Act	33
Part 2: Loop's obligations under the Data Protection Act	33
Defining Data Processing Activities	33
Ensuring Lawful Processing	33

Obtaining Consent	34
Transparency and Communication	34
Data Subject Rights	34
Data Security	35
Summary	35

## Part 1: Loop's need for a DPIA

Loop's independent online platform reinvents accountability in humanitarian aid and development by enabling communities to give feedback on services they receive, freely and safely.

Our goal at Loop is to make sure people can share their opinions and experiences on any issue that is important to them. It could be Thanks, a Request for Information, a Request for Support, a Concern or it may include sensitive issues. Sensitive reports are those that would do harm if they were posted on the open platform and include reports of Sexual Exploitation, Abuse and Harassment (SEAH); reports of Child Protection; Gender-based Violence (GBV); fraud or corruption allegations; other misconduct such as bullying and racism. Loop has invested heavily in a system whereby any sensitive feedback is channelled away from the open platform and handled safely and confidentially. Thus our priority is to make sure that people can give their feedback in a safe way, to improve accountability, keep people safe and ensure survivors receive the support they need.

Loop is accessible to all: online, or by SMS, WhatsApp, Messenger or voice via Loop's Interactive Voice Response and Reply (IVRR) technology, in local languages and provides a completely safe and anonymous channel for the reporting of sensitive feedback, all managed confidentially. It is therefore critical that Loop processes and systems adhere to the highest levels of data protection in order to keep people safe.

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 the individual, community and global level.

Data, Trust and Safety is at the heart of a functional Loop platform for it to add value to others, therefore analysing the Impact of Data Protection is ingrained in everything that Loop does, rather than an ad hoc project or process. Therefore this Loop Data Processing Impact Assessment is a live document being updated as we assess impact and implement new features.

This DPIA relates to the Loop platform, open and sensitive feedback. That includes any feedback received which goes to the Loop open platform and statistics page, from any country, through any channel and in any language. As well as any sensitive feedback which comes through any channel in any language and is sent to Sensitive Feedback Leads for referral and processing.

This DPIA is an open source public document, in line with our open policies and approaches and is available on the [Loop website](#) along with our [Codes of Conduct](#), [Privacy Policy](#) and other organisational information. It is open source because the safety of the data is important for individuals choosing to use Loop and for organisations wishing to use Loop to more effectively and efficiently engage, learn from and respond to local populations and also to access the open data confidently.

The impact of Data Protection and associated risks is an ongoing and integral part of the design and building of the Loop platform and all existing and new functionalities. With a functional product available and the main infrastructure built, we are writing up the process, findings and mitigation actions already delivered and will continue to review, reflect and improve on this, on an ongoing basis with every new functionality, country and user experience from partners and key stakeholders.

Data protection is not only about hardware and software but also about policies, behaviours, culture and communication and feedback is invited on how to improve this document, our Data Protection methods and the platform itself. Please share any feedback with [alex@talktoloop.org](mailto:alex@talktoloop.org) to help us ensure the safest service possible.

## **Part 2: The Nature of Loop's Processing**

### **What is the source of the data?**

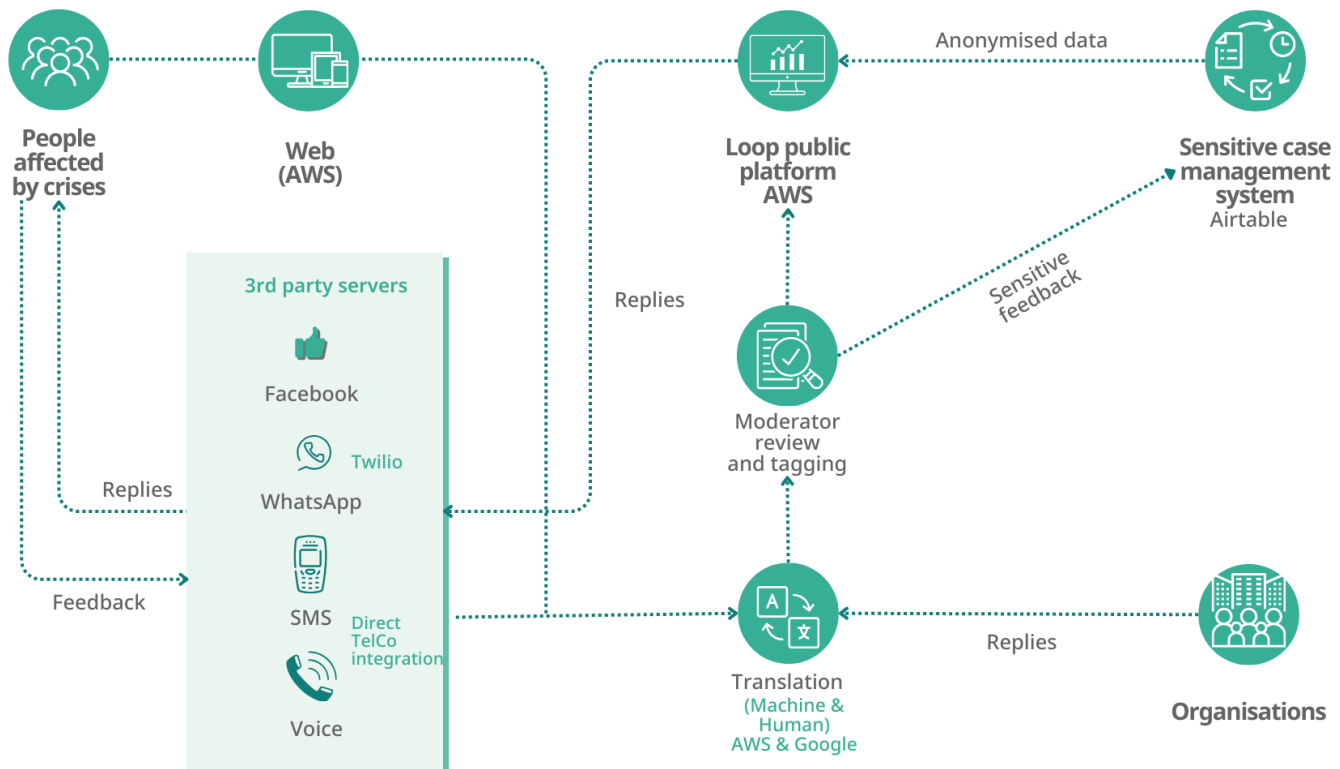
Loop collects data and feedback via our platform from any user, anywhere in the world. We work through a Charitable Franchise model where national organisations request to be the host of Loop in any given country. We then work together in partnership to build the appropriate products - languages, input methods etc - for their country needs and context.

The feedback is tagged by moderators, such as Organisations who might be able to respond to the feedback to offer help or support. The feedback is tagged by feedback Type (by the author or the moderator) and by Thematic area by the moderator to help

with analysis of feedback at an aggregate level. The author is invited to tag their feedback as sensitive or not. The Moderators can also add a sensitive tag but they cannot remove a sensitive tag if it is created by the author of the feedback.

The below diagram shows the flow of information from the two main Stakeholders (people affected by crises and the organisations they are feeding back on) and what information is used. The more detailed data is then outlined in the figure below:

**Figure 1: Loop's Data Flow Map**



## Who do we share data with?

The information from the feedback submitted which are NOT tagged as sensitive, are posted on the open platform of Loop and a notification is sent to everyone who engages with the content every time there is a new interaction to that feedback thread.

Sensitive feedback is sent to the Sensitive Feedback Leads and all data is removed from the Loop platform and moderators page. Only the Loop trained Sensitive Feedback Leads, the CEO and one tech team member can access the Sensitive Feedback Handling Tool hosted on [Airtable](#); it is a tool adapted to Loop's requirements and is GDPR compliant.

Users can only contact each other through the Loop platform, much like Twitter or Instagram. However, it first goes through a process of human moderation (unlike Twitter or Facebook) and does not post anything on the Open Loop public platform unless it meets the Loop criteria. This includes:

- 1) The [Community Guidelines](#) which are translated into multiple languages and dictate the type of online community Loop is trying to foster. These guidelines are linked from both the Loop website and platform, with a consent note. Any post which does not adhere to these guidelines is rejected by a Loop moderator and is not published on the platform.
- 2) The [Moderator Protocols](#) which are constantly updated based on learning and are open source, where we invite anyone from any community or organisation to make suggestions or discuss the Protocols guiding our decisions to post feedback or not.

We have included into our policies and processes that if people share too much information that might put them at risk, the moderators can either

- 1) tag it as a sensitive feedback to be sent to the sensitive feedback team to manage
- 2) reject the feedback and ask the author to resubmit in accordance with the platform protocols ensuring a safe, moderated space for all users
- 3) redact some aspects of the feedback - blank out phone numbers or last names for security purposes. The original feedback will remain on the Loop database but not be available for anyone else to see. There are strict guidelines around what can and cannot be redacted with the integrity of the feedback and safety at the core of all decisions.

## Data Collection Minimisation

The only data an author **must** share to submit a feedback on Loop is the feedback itself, of 8 characters or more. There are also options to share additional details about the feedback and/or author. These are all opt in and optional and are listed below. This “opt in” policy is how we minimise personal data collection, giving users full control and decision over what data they wish to share or not.

Someone (in or outside of an organisation) who is submitting a reply also only needs to write 8 characters or more and can include their reply contact details or choose not to.

We chose to only request the minimal data points (age groups, gender, disability according to the Washington Definitions) even though organisations requested Loop to gather additional data points such as legal status, race, ethnicity etc. We only do this if it is voluntarily included in the text of the submitted information.

- We will only store voice recordings for the minimum time required to be able to respond to any queries about the submitted feedback through IVRR. At the moment we have set this at 6 weeks but hope to reduce that to two weeks when our systems are well refined and tested.

## What “Opt In” data do we request & collect?

### Feedback details

#### Country

Knowing the country in which the authors are located helps us to understand the context of each feedback, more easily tag in relevant organisations who might be able to respond and provide better support. We automatically detect a user's country by using the IP address of the device and the author is given a choice to include it. They must consent for it to be included. The address can also be changed.

#### Location

Loop uses approximate location to encourage organisations near the author to respond to the feedback and provide support. Based on the location entered, we use the Google Places API to identify the closest village/town/city and then contact the local organisation to make them aware of the feedback and invite a response.

Information on precise locations are not stored or shared. We do not store geolocation; rather, we use runtime user geolocation for a geocoding which we round up to at least at city level to avoid possible user identification. This means that only approximate locations will be displayed alongside feedback if the author chooses to enter it.

#### Organisation

Users tagging an organisation in a feedback helps Loop encourage organisations to respond and thus close the feedback loop, incentivising further feedback. A registered organisation that gets tagged is automatically notified of the feedback and a non-registered organisation that gets tagged will receive an email from the moderator, inviting them to join and respond.

This helps Loop show who is listening and responding to feedback.

Authors can identify the organisations to which they intend to direct the feedback and Loop or anyone else can tag in or suggest other organisations that might be interested in or be able to help answer the feedback.

## **Author details**

This data allows organisations to see who is being listened to and better understand who is not able to share their voice and experiences and feedback. Then better targeting of activities to better listen to marginalised voices can take place.

### **Name**

This helps to make any interactions more personal or to see common feedback from the same author. Authors can choose to share their full name, use a nickname or remain anonymous. If they share a name, it is displayed alongside the feedback.

Moderators can redact some aspects of the name if this puts the author at risk (ie: remove the last name). This is assessed differently in each context with relevant country level guidance.

Names of staff or organisations are input by the individuals themselves and are stored in Airtable only. This is because they would like to be notified if their organisation is tagged in a feedback. This is optional.

Only the Data Owner and Data Processor have access to these names.

### **Phone number**

Providing a phone number is important so that the replies to the original feedback can reach the authors and the feedback loop can be closed. It removes the extractive nature of some feedback mechanisms.

If an author shares their phone number and consents to being contacted, we will notify them when/if anybody replies.

Phone numbers are stored on the Loop encrypted and separate database and are not available to any user or moderator. They can only be seen by the Data Owner and Data Processing Manager.



Numbers are never published online, and we will never share phone numbers from open feedback with anyone. Other users can only contact an author by using the Loop platform.

If it is a sensitive feedback, the Sensitive Feedback Leads can see the phone numbers once it has been sent to Airtable. All data is removed from the Loop Moderators platform. Authors are asked if it is safe to contact them back. Their response appears in Airtable.

If an author includes their phone number in the main text of their feedback, the moderator can 'unpin' the information or redact the number from the main text of the feedback before posting it. The original feedback is saved on the system but not available for the public.

Individual phone numbers related to an individual feedback that has been sent to the Airtable are shown only there and only Sensitive Feedback Leads have access to them.

Phone numbers of organisations are input by the individuals themselves and are stored in Airtable only. This is because they would like to be notified if their organisation is tagged in a Feedback. Organisations can share their email and not a phone number. This is optional.

Only the Data Owner and Data Processor have access to these phone numbers.

### **Email address**

Similarly, providing an email address is important so that the feedback loop can be closed to authors and they can be included and participate in ongoing discussions. It removes the extractive nature of some feedback mechanisms.

If an email address is provided the author will be notified of replies. They can unsubscribe from these notifications at any time. The email address is not published online, and Loop will never share the email address with anyone. People can only contact an author by using the Loop platform.

Email addresses of organisations are input by the individuals themselves and are stored on Airtable only. This is because they would like to be notified if their organisation is tagged in a feedback.

Only the Data Owner and Data Processor have access to these email addresses.

## **Data which is tagged:**

### **Physical or mental health condition**

People who have a physical or mental health condition are often treated differently. If we know about this, we can try to find a specialist organisation that can better meet their needs. We also display this data on our statistics page from tags placed by the author or moderators. Data used on our statistics page helps people and organisations understand who is using Loop and what their specific needs and experiences are. It helps organisations target these lesser heard populations more specifically to better meet their needs.

We follow the approved Washington Definitions for the tag names and we ask if someone self identifies as having a disability. If they choose to disclose this, the tags they choose are added to their feedback. These include:

- Seeing
- Hearing
- Mobility/Dexterity
- Learning/Understanding
- Selfcare
- Speaking
- Other

### **Gender**

People of different genders are often treated differently and require different types of support. If we know about this, we can try to find an organisation that can better meet their needs. We display an overview of gender data in our statistics page from tags added by authors or moderators. The options include:

- Female
- Male
- Non binary
- Prefer not to answer

### **Age**

People who have different ages are often treated differently. If we know about this, we can try to find an organisation that can better meet their needs. We display an overview of age data in our [statistics page](#) from tags added by authors or moderators. The options include the following age ranges:

- Between 14 - 17
- Between 18 - 29
- Between 30 and 59
- 60+

- Prefer not to answer

Feedback from children under 14 is treated as sensitive and removed from the Open platform. Moderators tag it as “sensitive” and refer it to the Sensitive Feedback Leads.

## Data Download

Loop’s Data Download Service allows users to export open feedback data in CSV format, enabling detailed analysis and custom report creation. It includes automatic data extraction via API for seamless integration with existing systems, providing real-time access to feedback data. The downloadable data is a replica of the information on the open platform, excluding sensitive information and Personally Identifiable Information (PII). This service enhances data management for more effective community engagement.

## Who is responsible for keeping Loop data safe?

The Managing Director of Loop is the Data Owner. She reports to the Governing Board every 2 months and this includes reporting on the data management risks, which are stored on the Loop Risk Register, which includes risks on Data Protection, reputational damage, partnership approaches and others.

The Loop Risk Register is a spreadsheet that is accessible and available for all Loop staff to contribute to and comment on and is reviewed every 6 months.

The Loop Moderators and Country Leads are employed contractually by the host organisations in each country.

Loop Sensitive Feedback Leads and User Experience and Quality Assurance Lead are employed directly by Loop.

All staff, consultants and partners sign the Loop Policies and Codes of Conduct which include confidentiality requirements. They also attend Safeguarding training and Data Management Training which covers the Loop Data Management Policies.

Loop’s Senior Platform Team consists of the CEO (Data Owner), Data Processor and Loop’s Technology Lead. This team is responsible for managing and making decisions on data safety, storage and access.

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

Loop is constantly learning and we aim to deliver on the [Privacy by Design approach](#). To keep the platform safe and secure we execute monthly security maintenance reviews and internal audits. For any new features we implement external audits to verify and identify any potential vulnerabilities that were not already identified by the designers and developers. This includes ongoing penetration testing.

There is a [Code of Conduct](#) that all Loop staff sign and this contains provisions on confidentiality and the handling of data. We have discussions on confidentiality with all Sensitive Feedback Leads who have additional access to data - specifically the sensitive feedback. All Sensitive Feedback Leads have attended high level training and are professionals in the area of Case Management, Safeguarding, etc.

All Moderators and Sensitive Feedback Leads and consultants who have signed a Non Disclosure and Confidentiality Agreement, have talktoloop.org email addresses and only have access to shared Loop documentation through this email address. Moderators must only use talktoloop.org emails when exchanging anything about sensitive feedback. This is part of the onboarding and induction process and revisited during Data Privacy training sessions.

## Where do we store our data?

We store all of the above data on the Loop database, hosted on AWS in Frankfurt Germany (in the European Union) and as such our storage methods align with GDPR guidance. The AWS infrastructure provides security levels through their infrastructure. Additionally we use encryption at the database level as a further measure of data security.

Additionally, as mentioned, we store and handle sensitive feedback data on Airtable, which is GDPR compliant.

We encrypt all the data we store; nobody apart from the Senior Platform Team can access the information. Phone numbers and emails can be accessed by the Senior Platform Team only and, where required, the designated Sensitive Feedback Leads to process sensitive feedback and address appropriate services.

We use the following services to host data and files that enable Loop to run:

- ❑ **Amazon Web Services (AWS) (Amazon Web Services, Inc.)**

AWS processes Loop's data in Frankfurt, Germany. Processing data includes collecting, recording, organising, storing, adapting, using, making available, erasing or destroying personal data. For more information visit the [EU website](#). The AWS [Privacy Notice](#) is amongst the best and most transparent that was reviewed. They state, with respect to content, that customers wholly own their own content. AWS never accesses our content without consent and does not derive information from it. We also remain the data controller for our content. All the services that Loop is using with AWS are compliant with ISO 27018:2019.

□ **Amazon Simple Email Service (Amazon)**

We use this service to send account activation emails so people can set up a password to their Loop accounts. Read more about the Amazon Simple Email Service [Data protection in Amazon Simple Email Service](#).

□ **Brevo**

For other email communications we use the Marketing Platform of Brevo, a CRM suite. Brevo is [GDPR compliant](#). Their [Privacy Policy](#) is clear that they do not share data or contacts outside of legal situations where they have no choice.

□ **[Cookie policy](#)**

TalktoLoop.org uses trackers, including cookies. Loop only uses trackers directly managed by us and which are strictly necessary for making the platform run. We do not allow any third party trackers, so advertisers and analytic systems do not track Loop data.

□ **Airtable**

The Airtable [Privacy Policy](#) is clear and detailed. We have opted out of advertising and google data collection. Airtable actively deletes personal information that belongs to children.

- We use an Airtable database tailored to Loop's needs for sensitive feedback handling.
- We use an Airtable database to gather email addresses of organisations wishing to be notified by Loop of new feedback. We store names, emails and phone numbers from consenting people.

All Airtable data is only accessible to specific Loop staff, via two factor authentication.

## ☐ **CloudFlare**

Cloudflare have a very strong reputation for insulating businesses and organisations from attack. Their [Cloudflare Privacy Policy](#) is very clear that they do this without compromising data.

We use Cloudflare as an additional security to protect the platform from Distributed Denial of Service (DDoS) attacks. It brings many additional security features.

## ☐ **Microsoft**

We have limited our third party activities with Microsoft due to their lack of transparency, fragmented nature of sharing enough relevant information relating to data sharing or data processing.

## ☐ **Google**

We limit our use of Google to [Google Workspace](#) for internal email and internal shared file storage among Loop staff.

We manage Loop accounts here to ensure staff access to Loop files and services is managed from a single central location.

## **Email addresses and phone numbers are stored:**

- In the Loop system Database - this is used by the system to automatically notify users when a feedback is published/rejected or when a reply to a published feedback comes in and is also published.  
Only the Loop Data Owner and Data Processor have access to these.
- In Airtable for SignUp processes -we store emails, phone numbers and names, if they choose and consent to sharing them, to create Loop accounts for the user.  
Only the Data Owner and Data Processor have access to these.
- In the Sensitive Feedback Handling System - created in Airtable - to process sensitive feedback.  
Only the Loop Sensitive Feedback Leads, Data Owner and Data Processor have access to this.

For additional security we have enabled two factor authentication for AWS and for Airtable.

## **What data do we share?**

If there is a request for data to be shared, this is only done with informed consent of the author and all involved. Informed Consent is a requirement for sensitive feedback

referrals, and it is requested privately (not on the Open Loop platform) and is attempted using any contact method that has been shared with us (email, phone, text). If there is no response from an author, we do not share the requested information unless we assess a potential risk, in which case an individual risk assessment is carried out by a Sensitive Feedback Lead in conjunction with the Loop Managing Director.

We use this [data sharing agreement](#) when sharing data with partner organisations or we write an organisation specific Data Sharing Agreement if that is easier, ensuring it aligns with our existing approaches.

## Information Quality and Accuracy

Moderators are national people who can identify local nuances. Loop is hosted within a national infrastructure to tap into networks of local actors with knowledge and contacts to support the roll out and referral mapping for Loop.

If an individual states that they are registering as an employee of an organisation we review the shared information; information on the web and within our networks to authenticate that the email address/person is associated with that organisation. We may also email the individual asking for evidence. This is not a foolproof process as many staff working for small local organisations do not have work emails and their organisation does not have a website but operates through a Facebook page.

We have monthly Moderators training across the country teams to learn from each other, train on new improvements to the technology, and ensure a consistent high standard of moderation.

We can pull down posts to be moderated again or rejected if an issue is flagged or if more information comes to light, at any time.

We constantly improve and update the platform, based on learning and improvements to the technology. For example we implemented a way to retract information, based on the country risk factors, to ensure no PII is posted. The technology identifies if there are too many posts coming from one IP address and blocks it. Moderators reject repetitive submissions or strange patterns of posting feedback and rejects these where appropriate, explaining why.

## Data Access, Retention & Deletion

Anyone can request us to remove, change, re-tag or delete completely, anything that they shared. This is done by moderators and then sent to the Data Owner to address data update requests.

Anyone can also request us to remove a post that they did not write if they feel that it does not meet the Community Guidelines, Moderator Protocols or could do harm in some other way. These requests will go to a Sensitive Feedback Lead to review and implement or reject with a reason based on each individual context and against our SOPs which are informed by our mission. The author and requesting actors' views, among others, will be sought. As a result of such requests we will review our Policies and improve them if needed.

Loop will display people's feedback and the data associated with them (time stamps and tags) for as long as Loop exists. This is because longitudinal, qualitative data is important to look at trends over time and changes in what local people have chosen to share. This can help to inform what works, what is funded and what needs additional funding and attention. We delete phone numbers and emails when they will no longer be needed to provide services to the author (e.g. when a case is concluded).

If Loop ceases to exist and no longer pays for Amazon Web Services to host the platform, we may export or download data to be stored safely for as long as is legally required and then delete it permanently.

## Part 3: The Consultation Process

### Stakeholder Groups

Loop has three key stakeholder groups:

- 1) Community members including people affected by crisis
- 2) Organisations working to help people affected by crisis
- 3) Donors and any others wishing to use the data in their work and decision-making processes - research, policy, advocacy etc.

#### **Community Members and People Affected by Crisis**

Loop has consulted with people affected by crises in Somalia, the Philippines, Zambia and Ukrainians in Poland. In each of these populations we hired external facilitators through national tech organisations or used our own local staff to manage feedback sessions in the local language(s).



Going forward we will always use this model of listening to local voices and experiences from a wide cross section of society through safe locally managed processes.

We also had input four times per year from the [Loop Governing Board](#) who come from affected communities and were invested in Loop's success, representing for example: Yemen, Zimbabwe, Uganda, Syria, Palestine and The Philippines.

In each country many people were consulted and represented:

- all age groups (from 14 up to 70),
- genders (including LGBTIQ+ communities in countries where it is illegal),
- disabilities
- Internally Displaced People (IDPs), refugees and host communities
- ethnic minorities or persecuted communities
- rural and urban communities and camps (IDPs and transit centres)

We also sought information from people affected by:

- human rights abuses
- poverty
- exclusion
- gender-based violence
- emergency response and sudden onset disasters
- conflict, etc

This feedback then informed our prototyping and approach to the design of Loop. We went back to some communities again for second and third rounds of feedback on the resulting design of Loop. This always included (but was not exclusive to) people wanting to report open as well as sensitive feedback; i.e. vulnerable or marginalised populations.

With regards to data protection, we found a widespread concern about the risks of being identified by NGOs or those providing services in case there were negative implications for them (being taken off the list, abuse etc). In addition there were concerns that some community members might know their information and this could cause a negative impact on them.

We built the anonymity and opt-in (rather than opt-out) approach to data sharing as a result of this. It may result in less demographic information but puts the user's needs first.

We also built the second line of defence through hiring national moderators, who review all content before it is published on the Open Loop Platform, to help manage risks that the author may not identify themselves. They can redact some content (phone number, last name for example), or reject it and send it back to the author with an explanation of the reason for rejection. It also reinforced the need to maintain local human moderators and not move to AI for moderation completely.

The ability to feedback anonymously had the strongest positive reception in every country for local people of all types.

### **Accessibility**

Loop has had a third party expert group, run by people with accessibility issues, audit the usability and accessibility of the Loop website and platform. Our accessibility was audited against the WCAG 2.1 AA compliance, please see [Web Accessibility Initiative](#) for details.

The WCAG 2.1 AA compliance is useful for people with additional technology to help them engage with the digital online space. Loop also considers accessibility for those people who have difficulty accessing technology due to illiteracy reasons, having to borrow a phone, no access to smartphones etc. Those who may not have the resources for enabling technology. There are currently no standards for this but it is the prime focus for Loop as we grow and develop.

We have built an Interactive Voice Response and Reply (IVRR) technology to enable people who are not comfortable expressing themselves through SMS or typing.

We will integrate systems that support text-to-speech features ('Read to me' button) to increase accessibility of the service to non-literate, non-digital or those with limited accessibility to technology for other reasons such as disability.

### **Organisations working to help people affected by crisis**

In the design process we also consult widely and frequently with staff at various levels (governance, legal, communications, project staff, fund writers, risk management, tech, innovation, operations management etc) of the following organisations, including:

- Civil Society Organisations (CSOs)
- Grassroots activists
- NGOs
- Networks
- INGOs

- UN staff
- Think tanks
- Universities
- Technology leaders
- Government Authorities
- Private sector organisations
- Organisations providing feedback mechanisms and data analysis

We consulted these actors in the Philippines, Indonesia, Zambia, Somalia and Poland as well as Uganda, Yemen, Paraguay, and regional (Asia, West Africa, East Africa, Middle East, Pacific) and global headquarters. We also recruited key people onto the [Loop Advisory Board](#) who hold relevant positions in the humanitarian landscape, volunteer to share their thoughts and opinions with us and who are invited to give their input three times a year to Advisory Board meetings.

We found a widespread concern about the risk of complaints or allegations against organisations and questions about the authenticity of authors of feedback. As a result we enabled the moderators to reject feedback, and wrote the [Community Guidelines](#) and [Loop Moderator Protocols](#) to ensure a safe space. These tools are open documents and we invite feedback to build trust and improve them.

We enabled the sensitive feedback process where the data is removed from the platform for allegations or feedback that might do harm to an individual or organisation. This risk is carefully assessed by Loop Moderators and Sensitive Feedback Leads on a case-by-case basis. All of the data goes to Airtable.

There were also concerns about attribution of issues that communities raise and if local actors would take the brunt of the criticism when there is a whole decision-making chain and budget allocation process which involves more than one actor. For this reason we did not use a star rating system but instead used the 'Feedback Type' filters. This means that the statistical analysis shows the overall sentiment and pattern of feedback across different demographic groups.

Also, we track response rates, are organisations replying and if so how quickly. If they are replying and the quality of their responses. This gives the organisation a fair chance of response, explanation and to protect their reputation.

There was a wish from many to be able to measure the impact and to evidence the value of getting feedback. We included in the statistical analysis a way to see how many replies (from individuals or organisations) there have been and with what delay. This is to reinforce research showing that it is not about the amount of negative

feedback that you receive but more important is whether you respond, how quickly you respond and how you respond.

In the short term future, we plan to be able to tag replies based on their 'impact' - was information provided, was a referral made etc - and have this on the statistical analysis page, resulting in some possible impact information.

Longer term we would also like to use the platform to track what the original author thought of the feedback and their opinion on the impact of sharing their feedback. But how to do that in a way that cannot be gamed is to be determined.

We also designed a system to incentivise providing feedback even if you do not get a direct reply to your feedback from the tagged organisation, by openly tracking views, any replies from anyone and by having an upvote system.

### **Donors and others wishing to use the platform's open data in their work and decision making processes - research, policy, advocacy etc**

We spoke to:

- Donors
- Universities
- Standards agencies
- Specialist organisations working on feedback, accountability and reporting mechanisms - Feedback Labs, GTS, Integrity Action, Upinion, Care Opinion, REACH, Interpol, Resource Hub...
- Loop Advisory Board who could input three times a year collectively and at key moments
- Special workshops with key members of FCDO and the Safeguarding Unit and associated teams

This broad group's interests were primarily on accessibility to the filtering process and safely seeing both the qualitative and quantitative data to help inform analysis and extend the potential impact of the available data. It highlighted a wish to get access to the data from sensitive feedback and be informed about any reported issues.

Interestingly donors felt that they would want to know and large organisations felt they should know about their downstream partners but they did not think Loop should be informing or sharing any information about their own data and sensitive reports. They said it was their own responsibility to manage communications with upstream donors safely and in accordance with their donor and other legal

requirements. This was discussed at length with a variety of key actors, including Donors, large INGOs, small NGOs and others.

It was finally concluded that the confidentiality of the allegations and reporting of sensitive feedback was considered not to be the responsibility of Loop as a neutral trusted platform and that the aggregated data on the [statistics page](#) of the platform would show trends by organisational type (not by individual organisation) which anyone could act upon but would not have an impact on any one organisation. We had many iterations of how to classify this data and what and who would elevate any concerns if they were not being addressed. The Accountability Flow was designed to help address this and incentivise accountable management of reports but this is still to be tested.

Loop intends to continue to learn from, consult with and improve our approaches with inputs from a wide range of users on an ongoing basis and at key points in time: new features added, new countries etc.

### Testing of the Loop Systems (Audit)

We contracted Professor Mick Grierson, Research Leader, Creative Computing Institute from the University of the Arts, London and his team to review the Data security of our platform. These were his final recommendations on the 22nd of March 2022.

*'We have run a battery of tests, including several different scanners, across Loop's systems, and examined the code for potential vulnerabilities. It took a couple of days.*

*We're confident that our tests found no significant vulnerabilities. Our system scans reported several issues where there could be potential risks, but after checking these manually they almost all look like low risk / guidance level, and not significant or high risk. We weren't able to penetrate the application or destabilise it significantly.*

*The main security improvement I would recommend would be that at times, developer credentials are hard coded into the codebase. On one occasion, the username 'admin' appears in one of the source files, and it would be better if the team could avoid hard coding / using default usernames, and double check that they're not leaving any traces with their API keys etc.'*

### Methodology:

Mick and his team performed security analysis based on the Open Web Application Security Project®(OWASP) top ten standard awareness procedure, with additional server and infrastructure investigation. This procedure prioritises the top ten security

issues as indicated by OWASP as follows: access control, cryptographic failure, injection, design security, misconfiguration, components, authentication, software / data integrity, logging failure, and server-side request forging. They implemented:

- Analysis of IAC structure
- Service scan
- SAST (Static Application Security Testing) scan
- Result filtering (elimination of false positives)
- As the source code is predominantly in JavaScript / Typescript, they used the following analysis tools when testing;
- Npm Audit,
- Yarn Audit,
- Horusec-NodeJS,
- Semgrep,
- Checkov and
- Owasp Dependency Check (v2.2)

They verified and cross-referenced these results using Insider security tools. Finally, they performed interactive testing of running source code using burpsuite.

Their service scan found that the system itself is robustly deployed and has necessary security protocols in place. No systems were compromised during our investigation.

Since this time we have done an AWS security audit and will continue to review and make improvements.

## **Part 4: Assessment of necessity and proportionality**

### **Legal basis for data processing and transfer**

The overall legal framework for our processing of Personal Data is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC with related regulation.

Other potentially important legislation that also informs data policies relevant for Loop include the Computer Misuse Act 1990 and the Freedom of Information Act 2004. This is because these earlier acts inform the GDPR and as a consequence the DPIA.

The Data Controller for the processing of Personal Data is Loop - a legally registered charity called Ourloop Stichting (RSIN [861193660](#)) that also has Equivalency Determination to a US Public Charity 501c(3). Loop is registered at The Hague Humanity Hub. Fluwelen Burgwal 58. 2511 CJ, the Hague. Any questions, concerns or breaches should be addressed to Alex Ross, the CEO and responsible person.

Any concerns not resolved can be reported to the Dutch Data Protection Authority (Dutch DPA) - Po Box 93374 the Hague, Holland.

Loop has done a legal assessment in Zambia as it felt necessary to do so due to some new laws there that were being pushed through the Government. These have since been overruled but at the time, we contracted a lawyer to do an assessment of our risks and exposure to these potential laws in Zambia.

We also did an internal review of Somalia legislation and will do so for each new country, including adjusting SOPs and approaches to contextualise sensitive referral thresholds etc based on country specific risks.

→ We will continue to keep an eye on new legislation at the national, regional and global level and conduct other specialised assessments when needed.

National laws may require Loop to reveal personal data upon a request of public authorities in certain circumstances. If this happens, Loop will inform the author, and we will only reveal data that they chose to share. This is articulated in the [Privacy Policy](#).

## How do we ensure the compliance of our Data Processes?

Loop has a set of comprehensive Policies including:

- [Safeguarding Policy](#).
- [Sensitive Feedback Handling Framework](#).
- Risk Management Policy
- [Privacy Policy](#)
- Disciplinary Policy
- Digital Management Policy
- [Cookie Policy](#)
- Complaints Grievances and Whistleblowing Policy, and our
- [Code of Conduct](#)

This includes, and is reinforced by our Community Guidelines and Protocols. All Loop staff and partners staff who have been granted access to the Loop Moderation platform have received training on the Data Policy which focuses heavily on the importance of confidentiality. They have all also signed the Loop Codes of Conduct and have training in safeguarding on a regular basis. We track compliance to these commitments.

Our Sensitive Feedback Leads and User Experience and Quality Assurance Lead monitor the feedback of the country with whom they partner on an ongoing basis and use this to make improved tags and to design training to address any potential risks. The policies are updated based on learning on a regular basis.

We have a User Experience and Quality Assurance Lead who manages the quality and consistency of the Loop sites (web and platform) and checks through posts on the open site to ensure compliance. They have signed the same Codes of Conduct as other Loop staff. Any issues arising from this monitoring can be dealt with directly but learning on patterns or complex decisions are taken to the monthly Moderators training to discuss, agree and then reflect in the Moderator Protocols.

## Data Subject Rights

In line with data protection policies and legislation, people who have shared their personal data with Loop (data subjects) have a right of access to their Personal Data which we process about them. Anyone can write to Loop at [alex@talktoloop.org](mailto:alex@talktoloop.org) to request access to or amendment of the Personal Data that we have registered concerning them.

We also have a Safeguarding email address if needed [safeguarding@talktoloop.org](mailto:safeguarding@talktoloop.org). Or the Loop reporting platform can be used.

We will share people's Personal Data (only data concerning yourself, which you have given us yourself) in a structured, generally used and machine-readable format (data portability).

If people using Loop consent to share their data and they change their mind, they are entitled to revoke their consent at any time after proving their identity; 'the right to be forgotten'.

## Consent



'Informed consent' rather than just 'consent', is extremely important and as such the Loop [Privacy Policy](#) is available, translated and posters are printed and shared.

The Privacy Policy explains how data is managed at four different levels:

1) Pictorial for those less comfortable with the written word – translated

2) Short bullet points with topline information about what we do or do not do with people's information – translated

3) A longer document in plain english explaining where what data is stored and

4) A longer, more official Iubenda generated Policy with detailed legal aspects. This will be customised when funding permits.

Because Loop is an independent organisation and does not provide operational services we have removed possible pressures linked to the type of feedback they might choose to give. People can give feedback when they like from where they like. This came across as a very positive aspect of the design. It means that people do not feel pressured to say certain things in front of certain people.

The communication of informed consent is in all of the languages on the platform. It is reinforced by how Loop is introduced to people and also within the flow of the feedback people are given the choice to feedback but not have it published online.

We follow the [Guidelines for Industry on Child Online Protection](#) and if a child decides to give feedback but is less than 14 years of age we will treat the feedback like a sensitive feedback even if it is not sensitive. Our moderators consider the age of the author of the feedback when assessing relevant local risk factors.



- We will include in our monitoring and evaluation processes how people felt about the consent process and if they understood it and to get advice on how to better communicate it.
- We will also review other sites and how they request consent online to improve our own.
- Loop will not share personal contact information with anyone except for what is on the open platform, without the author's consent. We will seek consent from authors to share their information with specific verified contacts only.

## Part 5: Identify and Assess Risk

<b>Source of risk and nature of potential impact on individuals.</b> Include associated compliance and corporate risks as necessary.	<b>Likelihood of harm</b> (Remote, possible or probable)	<b>Severity of harm</b> (Minimal, Significant or Severe)	<b>Overall risk</b> (Low, medium or high)
<p><b>Appropriate Security measures</b></p> <p>We conducted some 'worst case scenario' planning with the Data Protection auditors as well as various local populations. We stress-tested our systems which were designed to mitigate these risks. The remaining, highest risks were:</p> <p><b>1. Authoritarian Governments or others trying to get access to Loop data</b></p> <p>Our highest risk was authoritarian governments wanting to get access to the data, or other targeted attacks to get access to the data. This was not considered likely in the short term but increasingly likely with scale.</p> <p>For this reason we decided to host Loop on Amazon Web Services (AWS) in Frankfurt. This ensured it met GDPR requirements and was protected by private sector security measures with constant investment.</p> <p>We also implemented multiple layers of security:</p> <ul style="list-style-type: none"> <li>□ At technical level by choosing:               <ul style="list-style-type: none"> <li>o Distributed Denial of Service (DDoS) protection service</li> <li>o Security by the infrastructure - AWS is our Platform as a Service as they provide multiple layers of security and invest to guarantee security</li> </ul> </li> </ul>	Remote	Severe	High

<ul style="list-style-type: none"> <li>o All communication between application's components is encrypted</li> <li>o All infrastructure elements are now IaaS, managed via terraform code.</li> </ul> <p>□ At domain level by:</p> <ul style="list-style-type: none"> <li>o Strict limitation of data access levels within the architecture design - only dedicated team members for specific sensitive user data</li> <li>o Two step verification for new members and organisations</li> <li>o All environment parameters are now stored in the AWS Parameter Store</li> <li>o Every environment has a dedicated VPC and no shared infrastructure components.</li> <li>o Development environment is hidden behind VPN access only.</li> <li>o Production and Staging environments are protected by CloudFlare.</li> </ul>			
<p><b>2. Staff accidental breaches</b></p> <p>Our next highest risk was data breaches from staff and moderators. As a result we improved our policies, processes and conducted training and mandatory induction training on data protection, safeguarding for all country teams and will have updates on a 6 monthly basis.</p> <p><b>3. Third party breaches</b></p> <p>The third highest residual risk was third parties access to Loop data and their management of this being out of our control. For example a</p>	Probable	Significant	Medium
	Probable	Significant	High

<p>Mobile Network Operator (MNO) in a given country reviewing the traffic on our site. All the data is open except for the sensitive feedback. We suggest people input sensitive feedback directly on our weblink to remove the number of third parties (WhatsApp, Facebook etc) but this is a choice by the author.</p> <p>We have vetted what third party actors we sign up with and have reviewed their policies. We try to remain working with those with the strongest policies (AWS) and have refused to work with some higher risk actors. This is a risk to all service providers.</p> <p>We have negotiated additional conditions with some third party actors.</p>			
--	--	--	--

## Part 6: Measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in part 5				
Risk	Options to reduce or eliminate risk	Effect on risk (Eliminated / reduced / accepted)	Residual risk (Low / medium / high)	Measure approved (Yes/no)
<b>Authoritarian Governments or others trying to get access to Loop data</b>	<p>Loop as an open feedback mechanism has less stigma than a Sexual Harassment app and is marketed accordingly to reduce risks.</p> <p>We will be looking at implementing tunnelling so that if a phone or computer is intercepted the history of the user having been on our site will not be evident</p>	Reduced	Medium	Yes

	<p>It is acknowledged that no amount of investment can guarantee against this risk but we can continue to review and make it harder to penetrate our systems.</p>			
<p><b>Staff accidental breaches</b></p>	<p>We have moderator training on a monthly basis and weekly country specific meetings to go over any specific scenarios. The Loop Sensitive Feedback Lead is the person overseeing the country partners' activities and approaches and brings in protection, GBV and SEAH management and country specialist approaches to each meeting. This close oversight enables quality oversight and builds a strong picture of national and emerging risks to manage. We also implement an alert system where sensitive feedback, tagged as urgent, sends an automated email to all Sensitive Feedback Leads to attend to the case in a timely manner without including any personal data in the alert.</p> <p>We have a User Experience and Quality Assurance Lead who reviews the platform and website and makes recommendations for immediate improvements to content as well as seeing patterns and raising issues in the moderation training.</p>	<p>Reduced</p>	<p>Medium</p>	<p>Yes</p>

	<p>Additionally, we run random and frequent quality checks on moderators' work, including rejected feedback and translations, to ensure that feedback is handled according to the different policies including this one.</p>			
<b>Third Party Breaches</b>	<p>As a result we have actively limited the number of third parties that we rely on.</p> <p>We prioritise translation within AWS so as not to involve another party where benefits are minimal. Sometimes the translations are better with alternative services and we assess the risk for each.</p> <p>Terms and Conditions and contracts for all third party services have been audited to confirm alignment with Loop's data security requirements. As a result we have negotiated additional Terms and Conditions with some third parties including MNOs and where this was not possible we have chosen not to partner with some actors. For example, Africa's Talking did not have sufficiently high enough levels of data security in their Policies.</p> <p>A full list of the actors that Loop works with can be found in the security analysis</p>	Reduced	Medium	Yes

	document from the Creative Computing Institute.			
--	---	--	--	--

Item	Name/date	Notes
Measures approved by:	Alex Ross	
Residual risks approved by:	Alex Ross	In each country we should attach an Annex of national relevant laws and considerations.
DPO advice provided:	Abe Shalash	DPO should advise on compliance with new initiatives.
Summary of DPO advice:		
DPO advice accepted or overruled by:	Accepted	If overruled, you must explain your reasons
Comments: Accepted		
Consultation responses reviewed by:	Abe Shalash	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	The Loop Digital Product Manager Abe Shalash	To be reviewed at whichever comes first: <ul style="list-style-type: none"> <li>• July 2026</li> <li>• if Loop enters a new country</li> <li>• if a need to review is identified</li> </ul>



## Annexes

### Talk to Loop Compatibility with Somali Law

Last updated: Aug 2025

This document compares Loop's DPIA which follows GDPR guidelines, to Somali data protection laws, specifically the [Somalia Data Protection Act](#) passed in 2023 to ensure Loop is acting within its legal obligations in Somalia when it comes to its data processing activities.

#### Part 1: What is the Somalia Data Protection Act

The Data Protection Act is a set of laws passed by Somalia in 2023 to account for the lack of data protection regulations. The laws lean on other data protection laws such as the EU's GDPR and California's CCPA and as such the general themes covered by the Data Protection Act are compatible with the EU's GDPR regulations.

Those sets of law apply to all organisations either processing personal data of data subjects of Somalia and hence it is important for Loop to ensure its processes are aligned with the responsibilities of data controllers as described in the Data Protection Act, and that the methods used to collect and process data do not infringe on the rights of data subjects as described in the act.

#### Part 2: Loop's obligations under the Data Protection Act

As a data controller, Loop's obligations under the Somali law can be broken down into:

##### Defining Data Processing Activities

As a data controller Loop has outlined its data processing activities within its [DPIA](#). As a summary, loop's feedback submission system will collect data submitted by data subjects through one of its channels. The data processing consists of transcription, translation, tagging, aggregation, and publicly posting the data submitted.

##### Ensuring Lawful Processing

As a data controller, Loop must ensure that all data processing activities have a lawful basis. Common legal grounds include the consent of the data subject, the necessity of processing for the performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest, or legitimate interests pursued by the controller or a third party. Considering that Loop is a feedback system, in which users use the system to report on matters that concern them, their well being, the good of the public interest, all data submitted to Loop falls under the category of lawful processing as described in the Data Protection Act Article 14 sub-article 2. Additionally, Loop adopts an open data policy in which its policies are openly accessible via the Loop website, complying with the Data Protection Act's Article 14 sub-article 1.

### **Obtaining Consent**

Loop collects its data directly from the data subject, with the subject's consent. Should the subject revoke their consent Loop has documented its data deletion processes within its DPIA above. Additionally on the Loop web app, any personally identifying data is submitted optionally alongside the feedback submitted, in an opt-in fashion, allowing data subjects to submit feedback to the system anonymously.

### **Transparency and Communication**

Transparency is one of Loop's values, and as such Loop's policies are made publicly accessible via the [Loop Website](#). Where possible and reasonable, Loop will educate the data subjects on the purposes of the data collection, the data processing carried out by Loop, and their rights.

### **Data Subject Rights**

In accordance with Articles 20-23 of the Data Protection Act, Loop will ensure data subjects can ask whether Loop holds their personal data, can ask for a copy of the data, can ask for the data to be corrected, and can ask for the data to be deleted. Additionally, data subjects can either object to Loop processing of their data, or withdraw their original consent for data processing, which would entail a deletion of their data. Finally Loop does not have any automated processes that profile subjects or produces a legal or similar significant effect on the data subject.

## Data Security

The data collected and stored by Loop is encrypted both in transit and at rest, and multiple security layers are put in place to ensure the security of the data submitted by the data subjects. The full measures put in place and the risks associated with Loop's activities as well as the risk mitigation methods are outlined within the above Loop DPIA.

## Summary

Somalia has passed a set of laws called the Data Protection Act, and in order for Loop to function legally within Somalia it needed to ensure its practices are aligned with the laws specified in this Act. Since the Data Protection Act laws are inspired by European GDPR laws, which Loop is already in compliance with, we've found that the current Loop policies, and Loop's DPIA are adequate for lawful functioning within Somalia.

Within the DPIA, Loop has outlined its data processing activities, its data security practices, and risk assessments and mitigation strategies making it compliant with Somali law as well as EU law. Additionally, Loop ensures data subject rights are respected, and proper consent is collected, while keeping the documentation transparent on the Loop website.