Collecting & Sharing Geo-Located Data in Crisis Situations

Decision-making tools for practitioners

Purpose

The decision trees that follow are meant to be used together with "Location-based data in crisis situations: Principles & Guidelines," produced by the Scientific Responsibility, Human Rights and Law Program (SRHRL) of the American Association for the Advancement of Science (AAAS). They build upon this document to further explore how geo-located data is collected and shared in crisis situations, and how it can be done so ethically. Consult the full set of principles and guidelines for more considerations around aggregation, storage, archiving and deletion.

To learn more about SRHRL, visit: https://www.aaas.org/programs/scientific-responsibility-human-rights-law

How to use the tool

- Follow the flow of questions, **answering truthfully!**
- **Potential stopping points** are indicated by a caution symbol, and are a darker shade. These points are meant to encourage you to consider how you might make more ethical decisions in your plan.
- If you reach a stopping point, **take some time to explore how you could alter your data collection and/or data sharing plans accordingly**—but don't be afraid to explore where different answers might have led you in the decision tree. Once you've explored the different ways you could have answered questions in that series, move on to the next so that you can continue planning your project.
- **You'll notice that stopping points happen quite frequently.** That's because data collection and data use in crisis situations is complex and presents a number of risks. Engaging in these activities ethically requires a number of safeguards to mitigate potential harm. The goal is to demonstrate the many points at which geo-located data processes could potentially put people and communities represented in harm's way without adequate planning.
- **This is not meant to be an exhaustive resource covering all potential scenarios,** but a starting point to guide your thinking around data collection and sharing in the context of crisis situations. Read the full principles and guidelines, consult with colleagues and do your own research to make sure that your projects are ethical and effective.

AAAS | Scientific Responsibility, Human Rights and Law

Should I collect location-based data in this crisis situation?

AAAS | Scientific Responsibility, Human Rights and Law

Considerations for Data Collection

Data Minimization

Once you collect something, it could exist forever. That means the risks of breaches, leaks and misuse could, too. Collect only the data you need, and make a plan for deletion, too.

Do No Harm

If you build projects without contextual knowledge or partnerships, you may unintentionally bring harm to the populations you're aiming to help.

Informed Consent

It's best to only collect data that individuals agree to share after they understand how their data will be used and what risks it might bring.

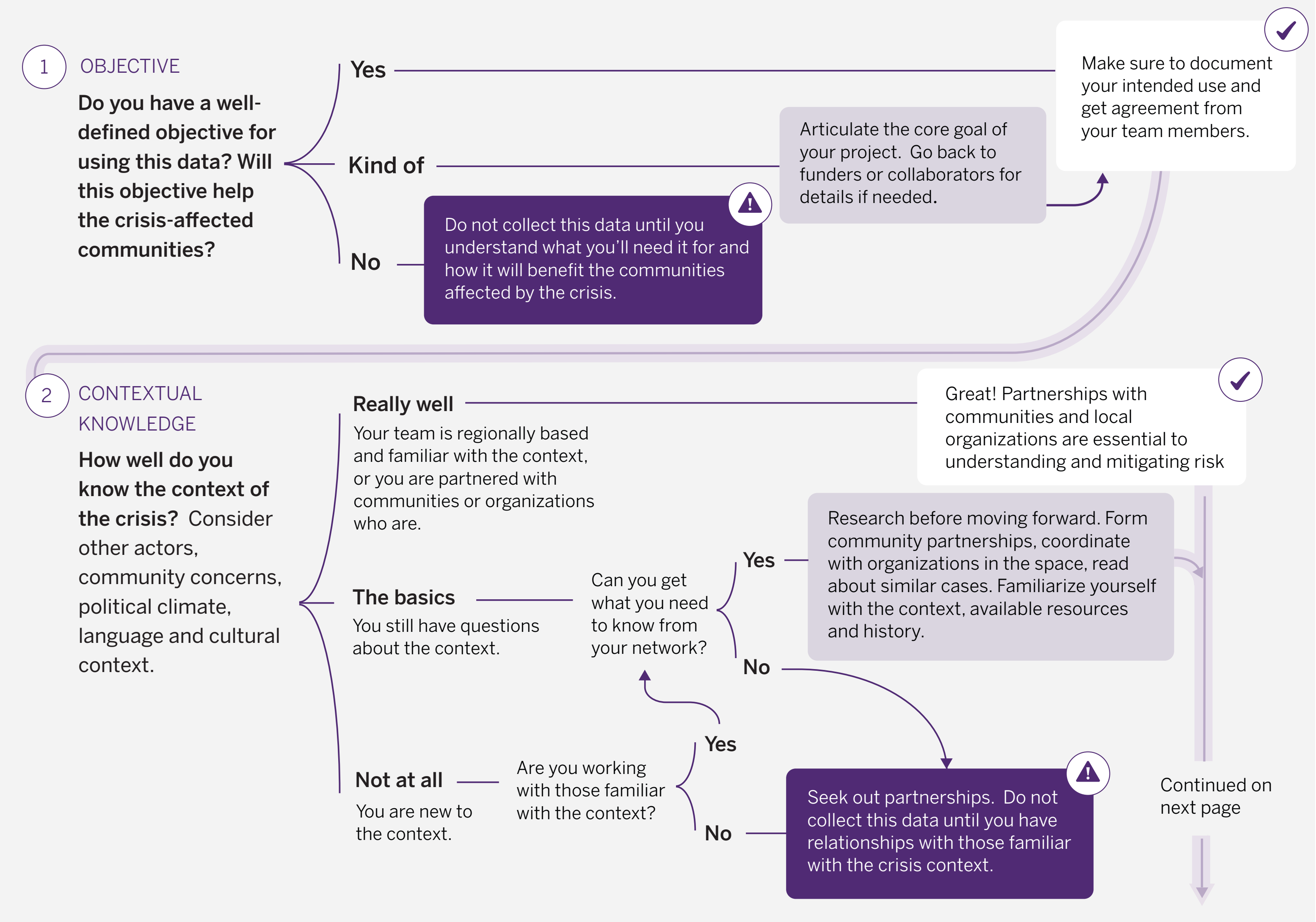
Anonymization

Identifiable information (e.g. names, home addresses, IP addresses, phone numbers) should never be provided. You don't need many data points to identify someone.

Train Volunteers

"Do no harm" applies to data collectors, too. Poorly collected data puts the data collectors, those represented in the data and your project at risk.

Decision Tree Guide



1 OBJECTIVE

Do you have a well-defined objective for using this data? Will this objective help the crisis-affected communities?

Yes — Make sure to document your intended use and get agreement from your team members.

Kind of — Articulate the core goal of your project. Go back to funders or collaborators for details if needed.

No — Do not collect this data until you understand what you'll need it for and how it will benefit the communities affected by the crisis.

2 CONTEXTUAL KNOWLEDGE

How well do you know the context of the crisis? Consider other actors, community concerns, political climate, language and cultural context.

Really well
Your team is regionally based and familiar with the context, or you are partnered with communities or organizations who are.

Great! Partnerships with communities and local organizations are essential to understanding and mitigating risk

The basics
You still have questions about the context.

Can you get what you need to know from your network?

Yes — Research before moving forward. Form community partnerships, coordinate with organizations in the space, read about similar cases. Familiarize yourself with the context, available resources and history.

No

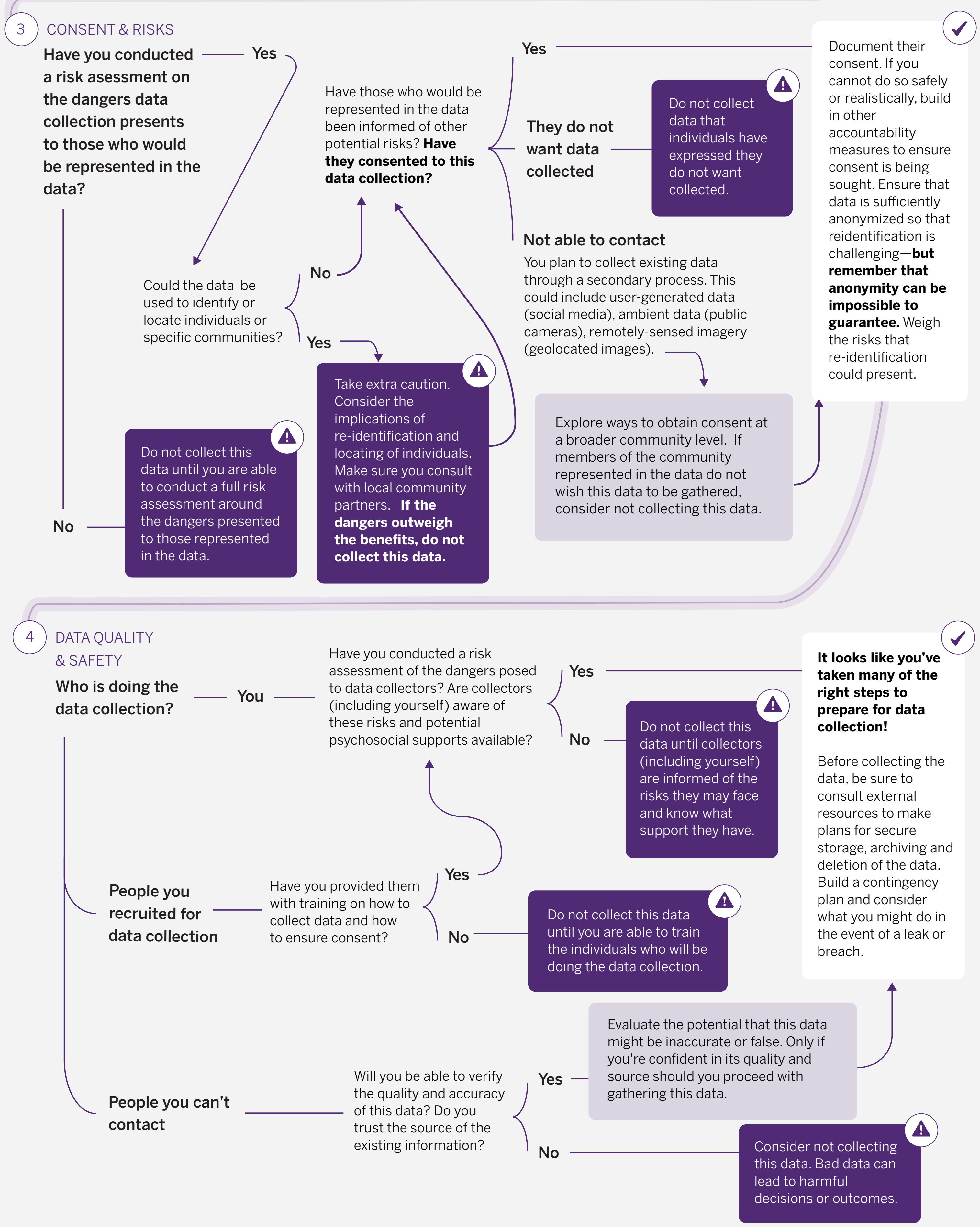
Not at all
You are new to the context.

Are you working with those familiar with the context?

Yes

No — Seek out partnerships. Do not collect this data until you have relationships with those familiar with the crisis context.

Continued on next page



3 CONSENT & RISKS

Have you conducted a risk assessment on the dangers data collection presents to those who would be represented in the data?

Yes

Could the data be used to identify or locate individuals or specific communities?

No

Have those who would be represented in the data been informed of other potential risks? **Have they consented to this data collection?**

Yes

Document their consent. If you cannot do so safely or realistically, build in other accountability measures to ensure consent is being sought. Ensure that data is sufficiently anonymized so that reidentification is challenging—**but remember that anonymity can be impossible to guarantee.** Weigh the risks that re-identification could present.

They do not want data collected

Do not collect data that individuals have expressed they do not want collected.

Not able to contact

You plan to collect existing data through a secondary process. This could include user-generated data (social media), ambient data (public cameras), remotely-sensed imagery (geolocated images).

Explore ways to obtain consent at a broader community level. If members of the community represented in the data do not wish this data to be gathered, consider not collecting this data.

Yes

Take extra caution. Consider the implications of re-identification and locating of individuals. Make sure you consult with local community partners. **If the dangers outweigh the benefits, do not collect this data.**

No

Do not collect this data until you are able to conduct a full risk assessment around the dangers presented to those represented in the data.

4 DATA QUALITY & SAFETY

Who is doing the data collection?

You

Have you conducted a risk assessment of the dangers posed to data collectors? Are collectors (including yourself) aware of these risks and potential psychosocial supports available?

Yes

It looks like you've taken many of the right steps to prepare for data collection!

Before collecting the data, be sure to consult external resources to make plans for secure storage, archiving and deletion of the data. Build a contingency plan and consider what you might do in the event of a leak or breach.

No

Do not collect this data until collectors (including yourself) are informed of the risks they may face and know what support they have.

People you recruited for data collection

Have you provided them with training on how to collect data and how to ensure consent?

Yes

No

Do not collect this data until you are able to train the individuals who will be doing the data collection.

People you can't contact

Will you be able to verify the quality and accuracy of this data? Do you trust the source of the existing information?

Yes

Evaluate the potential that this data might be inaccurate or false. Only if you're confident in its quality and source should you proceed with gathering this data.

No

Consider not collecting this data. Bad data can lead to harmful decisions or outcomes.

Should I share location-based data in this crisis situation?

AAAS | Scientific Responsibility, Human Rights and Law

Considerations for Data Sharing

Share With a Purpose

Ensure decisions about data-sharing are mission-driven and goal-oriented. Make sure that you have clearly defined use cases in mind.

Extra Caution in Conflict Situations

Data affiliated with conflict situations may lead to serious consequences for vulnerable populations if adversarial groups gain access to the data.

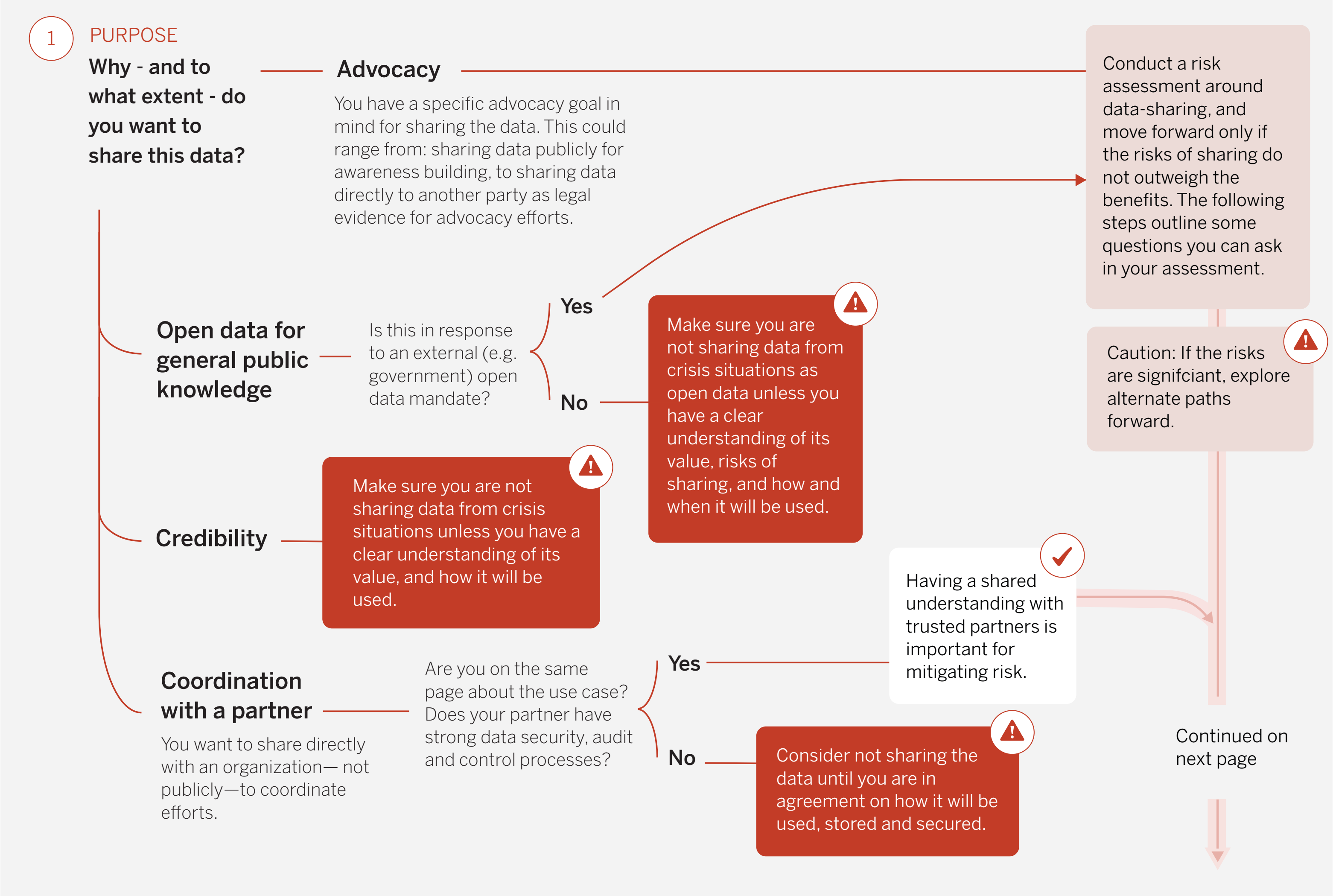
Manipulation and Misuse of Data

There are implications for sharing data, including the possibility that people will misinterpret maps and visualizations or actively manipulate and mis-use data in a way that leads to harm.

Stewardship and Knowledge Repatriation

Communities have a right to access data collected about them, as well any insights derived from these data. Meaningful engagement may require capacity-building around data literacy.

Decision Tree Guide



1 PURPOSE

Why - and to what extent - do you want to share this data?

Advocacy

You have a specific advocacy goal in mind for sharing the data. This could range from: sharing data publicly for awareness building, to sharing data directly to another party as legal evidence for advocacy efforts.

Conduct a risk assessment around data-sharing, and move forward only if the risks of sharing do not outweigh the benefits. The following steps outline some questions you can ask in your assessment.

Caution: If the risks are signifcant, explore alternate paths forward.

Open data for general public knowledge

Is this in response to an external (e.g. government) open data mandate?

Yes

No

Make sure you are not sharing data from crisis situations as open data unless you have a clear understanding of its value, risks of sharing, and how and when it will be used.

Credibility

Make sure you are not sharing data from crisis situations unless you have a clear understanding of its value, and how it will be used.

Coordination with a partner

You want to share directly with an organization— not publicly—to coordinate efforts.

Are you on the same page about the use case? Does your partner have strong data security, audit and control processes?

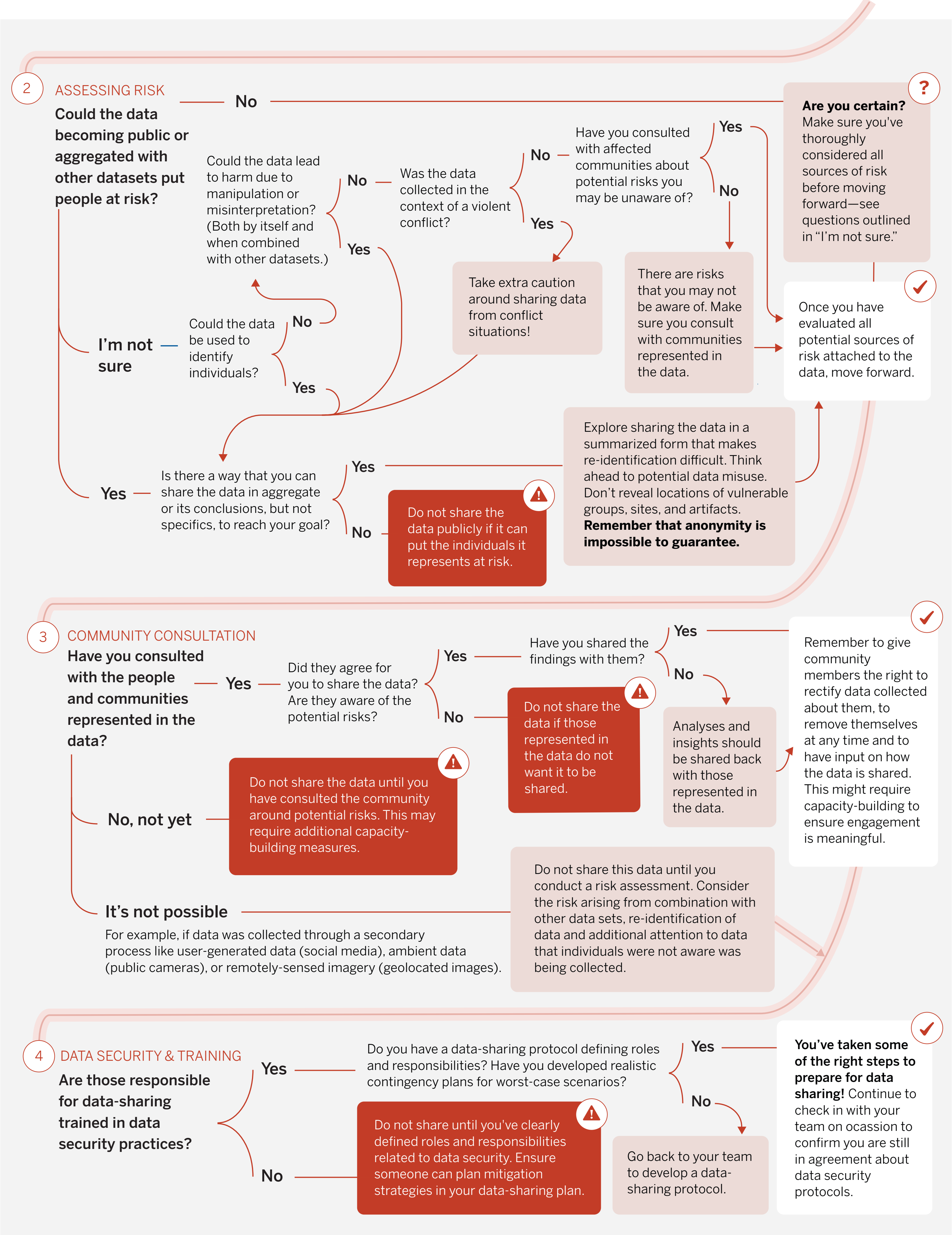
Yes

Having a shared understanding with trusted partners is important for mitigating risk.

No

Consider not sharing the data until you are in agreement on how it will be used, stored and secured.

Continued on next page



2 ASSESSING RISK

Could the data becoming public or aggregated with other datasets put people at risk?

No

Could the data lead to harm due to manipulation or misinterpretation? (Both by itself and when combined with other datasets.)

No — Was the data collected in the context of a violent conflict?

No — Have you consulted with affected communities about potential risks you may be unaware of?

Yes

No

Yes

Take extra caution around sharing data from conflict situations!

There are risks that you may not be aware of. Make sure you consult with communities represented in the data.

Are you certain? Make sure you've thoroughly considered all sources of risk before moving forward—see questions outlined in "I'm not sure."

?

✓

Once you have evaluated all potential sources of risk attached to the data, move forward.

Yes

I'm not sure — Could the data be used to identify individuals?

No

Yes

Yes — Is there a way that you can share the data in aggregate or its conclusions, but not specifics, to reach your goal?

Yes

Explore sharing the data in a summarized form that makes re-identification difficult. Think ahead to potential data misuse. Don't reveal locations of vulnerable groups, sites, and artifacts. **Remember that anonymity is impossible to guarantee.**

No

⚠ Do not share the data publicly if it can put the individuals it represents at risk.

3 COMMUNITY CONSULTATION

Have you consulted with the people and communities represented in the data?

Yes — Did they agree for you to share the data? Are they aware of the potential risks?

Yes — Have you shared the findings with them?

Yes

✓ Remember to give community members the right to rectify data collected about them, to remove themselves at any time and to have input on how the data is shared. This might require capacity-building to ensure engagement is meaningful.

No

Analyses and insights should be shared back with those represented in the data.

No

⚠ Do not share the data if those represented in the data do not want it to be shared.

No, not yet

⚠ Do not share the data until you have consulted the community around potential risks. This may require additional capacity-building measures.

It's not possible

For example, if data was collected through a secondary process like user-generated data (social media), ambient data (public cameras), or remotely-sensed imagery (geolocated images).

Do not share this data until you conduct a risk assessment. Consider the risk arising from combination with other data sets, re-identification of data and additional attention to data that individuals were not aware was being collected.

4 DATA SECURITY & TRAINING

Are those responsible for data-sharing trained in data security practices?

Yes — Do you have a data-sharing protocol defining roles and responsibilities? Have you developed realistic contingency plans for worst-case scenarios?

Yes

✓ **You've taken some of the right steps to prepare for data sharing!** Continue to check in with your team on ocassion to confirm you are still in agreement about data security protocols.

No

Go back to your team to develop a data-sharing protocol.

No

⚠ Do not share until you've clearly defined roles and responsibilities related to data security. Ensure someone can plan mitigation strategies in your data-sharing plan.