British Embassy Jakarta

GETTING TO GOOD HUMAN TRAFFICKING DATA

Everyday Guidelines for Frontline Practitioners in Southeast Asia

WSD HANDA CENTER FOR HUMAN RIGHTS & INTERNATIONAL JUSTICE
Stanford University

EAST-WEST CENTER
COLLABORATION · EXPERTISE · LEADERSHIP

HUMAN RIGHTS RESOURCE CENTRE

GETTING TO GOOD HUMAN TRAFFICKING DATA

Everyday Guidelines for Frontline Practitioners in Southeast Asia

Lead Researcher and Author
Jessie Brunner Program Manager, WSD Handa Center for Human Rights and International Justice, Stanford University

Research Support
Adhigama Budiman Researcher, Institute for Criminal Justice Reform
Cess Principe Research and Project Coordinator, Human Rights Resource Centre
Maidina Rahmawati Researcher, Institute for Criminal Justice Reform
Sovanna Sek Lawyer, Member of the Bar Association of the Kingdom of Cambodia

Administrative Support
Aiydinia Asyadamulti Finance Assistant, Human Rights Resource Centre
Olivia Christina Administrative Assistant, Human Rights Resource Centre
Juniati Suryadi Office Manager, Human Rights Resource Centre

The author would like to thank the numerous colleagues and mentors who provided guidance and support along the way, as well as informal peer review, namely:

Dr. David Cohen Director, WSD Handa Center for Human Rights and International Justice, Stanford University
Natasha Dolby Co-Founder, Freedom FWD
Dr. Kelly Gleason Data Science Lead, United Nations University
Laura Hackney Founder, Annie Cannons
Sarah Jakiel Independent Anti-Trafficking Expert & Consultant
Duncan Jepson Founder and Managing Director, Liberty Asia
Sophie Otiende Programme Consultant, HAART Kenya
Helen Sworn Founder and Director, Chab Dai
Penelope Van Tuyl Assoc. Director, WSD Handa Center for Human Rights and International Justice, Stanford University
Beth Van Schaack Faculty Fellow, WSD Handa Center for Human Rights and International Justice, Stanford University
Meredith Miller Vostrejs Prog. Manager, WSD Handa Center for Human Rights and International Justice, Stanford University

The development of this document would not have been possible without financial assistance from the **British Embassy, Jakarta**. The author would like to particularly thank **Rob Campbell-Davis** for his vision and support throughout the project. Additional support was provided by the **East-West Center**.

This report was designed and printed in Indonesia.

Layout & design by:
Basuki Rahmat (basuki.rekaimaji@gmail.com)

Roadmap

Foreword

This guide is the result of in-person interviews conducted over a period of three months with anti-trafficking practitioners from both government and civil society in four Southeast Asian nations, with additional input from international experts both on human trafficking and data management. **These meetings were aimed at identifying promising practices and understanding the most significant challenges for those people doing the critical day-to-day work – from investigating cases to serving survivors – of the anti-trafficking movement**. Those perspectives directly informed the content of these guidelines, making it tailored to the region of Southeast Asia, but widely applicable.

This guide is intended to serve as a reference document, offering baseline standards and recommendations based on current understanding around good, responsible data practices. The norms, laws, regulations, tools, and technologies relevant to data collection are rapidly changing; thus, practices will need to be revised and updated over time.

The information and recommendations outlined here are best understood holistically, meaning we hope readers will consult the full guide, while perhaps focusing on areas of particular concern to you and your team. Because **each individual and organisation working in the anti-trafficking field has distinct capacities, needs, and resources**, we recognise that this manual cannot be exhaustive or relevant for all actors, but we have endeavoured to cover key concepts that can be helpful to the most general possible audience.

This document was originally drafted in English and later translated into relevant languages of the region. As such, many of the resources referenced herein are unfortunately only available in English or accessible in restricted geographies. In continuing this work, the research team will aim to identify additional resources available in local languages. Note that any mentions of applications are not to be seen as an endorsement. Rapid changes in technology mean new tools are being developed continuously and others can become quickly irrelevant or outdated. It is always best to consult partners, colleagues, lawyers, and technical experts when selecting any new software or tool.

This guide is intended to serve as a reference document, offering baseline standards and recommendations based on current understanding around good, responsible data practices.

A caveat on the legal implications of data collection

This document aims to serve frontline actors carrying out the day-to-day work of the anti-trafficking movement in Southeast Asia, both within government and civil society. When discussing data collection, whether related to human trafficking or otherwise, one cannot ignore the issue of legal liability relevant to holding and using other people's data, which varies based on jurisdiction. In other words, these conversations about data are often set in an ethical framework of *should*, when in fact they also fall very firmly into the legal framework of *must*, and breach of a relevant law may create risk for your organisation, directors, and employees. Owing to the variance and technicality of legal frameworks across the region, this document purposefully sets these discussions aside in the hopes they will be taken up in the future by qualified entities.

What do we mean by **"Human Trafficking Data"?**

For many, the phrase "human trafficking data" brings the following statistics to mind: there are 40.3 million victims of human trafficking* in the world today, about three-quarters of them are women and girls, and the industry generates $150 billion in profits a year.

The global nature of these numbers, though undeniably important for advocacy purposes, can make them feel far removed from the day-to-day work of civil society organisations and government agencies at the frontline of the fight against human trafficking in Southeast Asia. But the reality is, each and every client you support, case you adjudicate, partner meeting you convene, investigation you undertake, and community outreach event you launch is essential to generating the data behind numbers like these.

It is also important to note that these statistics address only a fraction of the questions we need

40,3 MILLION
victims of human trafficking in the world today

Global Estimates on Modern Slavery 2017 (ILO, Walk Free Foundation, IOM)

ABOUT 3/4
of them are women and girls

Human trafficking generates
$150 BILLION
in profits a year

Profits and Poverty: The Economics of Forced Labour 2014 (ILO)

*Though the author acknowledges ongoing debate around preferred terminology, for ease, the phrase "human trafficking" will be used throughout to convey the international legal definition of "trafficking in persons" set out in the Palermo Protocol to the United Nations Convention against Transnational Organized Crime.

anti-trafficking movement:

a group of people with diverse skills and experience in advocacy, social work, research, activism, medical support, criminal investigation, fundraising, legal support, media outreach, and other fields working with the shared purpose of ending human trafficking and supporting survivors

trend :

a pattern of change or general tendency observed across data points

to understand to successfully combat human trafficking. **Furthermore, tailoring impactful policies and programmes to specific contexts – and being able to effectively evaluate that impact – requires high-quality, localised data.** This requires building a data-driven movement, which begins with each one of us – and these guidelines are intended to help us along. Our collective impact will no doubt be greater than the efforts we each make as individuals.

Only by starting at the local level can we begin to detect **trends** and understand systems of exploitation at a national or regional level. As emphasised in the recently adopted ASEAN Convention Against Trafficking in Persons, Especially Women and Children (ACTIP) and associated ASEAN Plan of Action, creating common data standards and practices, as well as opportunities to collaborate on data, will be a critical task in Southeast Asia as a hub of source, transit, and destination sites of human trafficking.

Unfortunately, both academia and the tech sector often struggle to make discussions around data inclusive to those outside these fields, in part through the use of highly technical language and specialized jargon. But these seemingly complex data concepts sound more intimidating than they actually are – and the anti-trafficking field has a lot to offer in these conversations. Not everyone needs to be a data expert, but we can all benefit – and

Words like **client, beneficiary, victim,** and **survivor** are often used interchangeably when in fact they have distinct meanings. These guidelines aim to be thoughtful in using the word that seems most accurate and appropriate in each context , though "victim" may be used when referencing a grouping of both victims and survivors for lack of a comprehensive term.

our work can benefit – from a basic level of awareness of data collection methods, data analysis skills, and data security awareness.

The truth is, we are constantly generating and collecting both **qualitative data** and **quantitative data** without even thinking. **Data are essentially just the building blocks of information, which produces knowledge, which we draw on to make decisions.** In the anti-trafficking field, these decisions can have a very direct impact on people's lives. Also, many of the issues that arise with data collection and management directly impact the human rights of **data subjects** so must be central to our work.

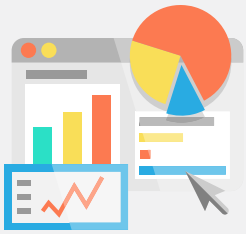
For all the talk about human trafficking data, there is very little talk about *good* data. **Good data should be thought of as the foundation of all anti-trafficking efforts** (See Data Principle #2). Good data can help us understand how to make awareness-raising campaigns more effective or how to better train community workers. They can help us understand the experience of a survivor five years post-trafficking or show what percentage of survivors are accessing holistic services in a given area, including psychosocial support and vocational training. Data can tell us what the average amount of restitution is in a certain jurisdiction or demonstrate how different regions are performing when it comes to trafficking cases reaching local courts – or how the very concept of human trafficking diverges across localities! **An often-overlooked aspect, data can give us valuable insight into how we are doing as an anti-trafficking movement.** Data offer us a way to measure performance in our daily duties or the strength of partnerships, and are critical to allocating resources efficiently.

qualitative data:

data typically gathered in a semi- or unstructured manner that describe something

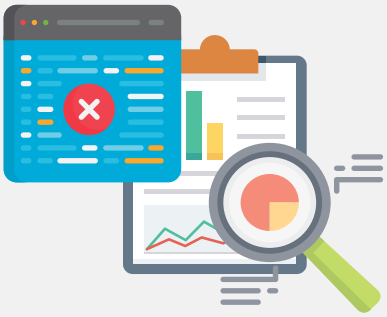
quantitative data:

structured, statistical data that measure something and can be expressed in numbers



data subject:

the person whose information is contained with the data; the person whom the data describe (Note: the term "data subject" implies more passivity that would be ideal being that this person is central to the conversation, but we use it here for its technical nature and lack of a better term.)



bias:

a preconceived notion or tendency about a given phenomenon; the introduction (often inadvertently) of an error into the process of data collection or analysis, which leads to faulty conclusions; a systematic overstatement or understatement of the true value of a measurement

In other words, our work should begin with questions, not data.

Good data maximise accuracy and completeness while minimizing **bias** and error, and are collected and analysed in a responsible manner that protects the people the data describe. Making critical decisions about programming, policies, and laws without data is likely to be inefficient and ineffective – and possibly even harmful. It is easy to imagine the consequences of acting on bad information.

As a movement, we need to rely more on data to support our intuitions, but that is not to say data are absent from our work. For example, many of us have comprehensive case files with family histories, migration information, health profiles, and other qualitative data critical to deeply understanding the nature of the problem. In other cases, technology has allowed for complex data processing, such as using satellite imagery to trace the movement of illegal fishing vessels or linking financial transactions to fraudulent bank accounts to catch traffickers and use their illicit earnings for restitution. But often the data that exist are limited, low-quality, or outdated. **There are entire groups of people who are not being counted.** This is in part a consequence of working with a hidden population. But it is also a consequence of not having adequate support and proper skills training on how to collect useful, actionable data and analyse what we do have.

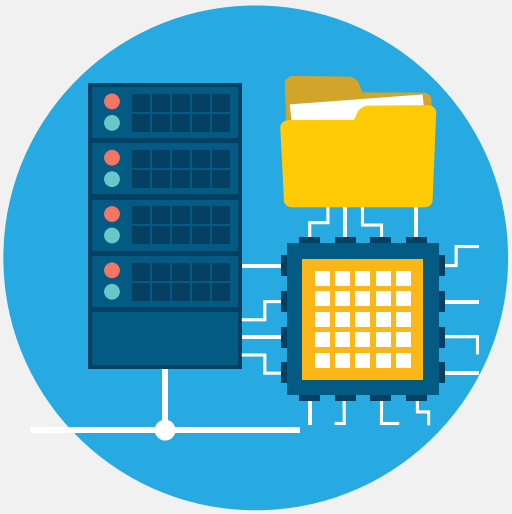
To propel our work forward, we need to focus on gathering data systematically and effectively, rooting all our work in the question of, "What do I need to know to support the movement to end human trafficking?" In other words, our work should begin with questions, not data. These could be questions about survivor reintegration needs; key geographic, demographic, and industry-specific vulnerabilities; effective prosecution tactics; or effective organisational strategies. From there, we can start asking, "**What do the data tell us?**"

To be effective, we will need to engage actors at all levels within a given organisation to be invested in data-driven programmes and systems. Chances are your stakeholders – whether donors, central governments, or multilateral entities – are pushing you for data anyway. **In addition to shaping your programmes, enhancing data systems in this way will make it easier and faster to meet reporting requirements.**

Much like the broader human rights architecture, there is no standardised framework governing the use of data within the anti-trafficking movement. This means it is up to us to set and follow norms and standards with regard to the collection, use, management, and analysis of relevant data in a way that enhances coordination while meeting the needs of each unique organisation. A great starting place is completing a landscape analysis of what peer agencies and organisations are doing and consulting the reference documents contained herein. **Of course, owing to the very different contexts and legal environments in which we all function, there can be no universal standard; however, this guide aims to encourage the development of a common understanding and set of general practices that enable us all to do our work more effectively, efficiently, and with an eye on protecting the privacy and safety of those we aim to serve.**

These guidelines aim to provide the necessary foundation to ensure the anti-trafficking community functions with good, responsible data at its core, with a particular focus on moving toward the systematic use of electronic or digital data. We begin with **seven core principles to support a data-driven movement** relevant to human trafficking before providing general guidance and practical tools related to **data ethics**, **data systems and databases**, **data storage**, **data security**, **data sharing**, **data analysis and interpretation**, and **data presentation and visualisation**. Each section begins with a short overview of the topic and goes on to offer specific practices and ideas that are illustrative of the broader issue. Remember, this is merely a starting place. It is recommended that practitioners consult additional resources, many of which are recommended herein, on the topics most central to their work.

To be effective, the data principles, norms, and recommended practices in these guidelines must be **integrated into every part of our work**, from deciding what information to collect on an intake form to selecting software for managing



These guidelines aim to provide the necessary foundation to ensure the anti-trafficking community functions with good, responsible data at its core, with a particular focus on moving toward the systematic use of electronic or digital data.

In summary, the answer for the anti-trafficking movement is not simply more data; it is better, more responsible data that goes far beyond annual donor reports or global statistics.

our data to developing ethics protocols to guide our work. As the anti-trafficking movement's standards and practices become more aligned, comparable, the picture of the problem will become clearer and we will become stronger. Data collected in different places by different people in different languages can be compared if gathered using similar methods and definitions. Over time, this allows us to look for trends and patterns of what makes people vulnerable to trafficking, what makes someone likely to be a trafficker, what the movement of illicit funds linked to trafficking looks like, what are common trafficking routes, and more.

In summary, the answer for the anti-trafficking movement is not simply more data; it is better, more responsible data that goes far beyond annual donor reports or global statistics. This is the only way we will get to the goals embodied in the ACTIP, namely to promote "stronger and more effective regional and international cooperation" through research, collection, sharing, and dissemination of accurate information. While acknowledging that the complexity of data as a concept makes it difficult to craft a guide that is relevant across the board, these guidelines aim to help anti-trafficking practitioners operationalise the norms and practices of good data. **By making an earnest effort to implement strong data practices, whilst being honest about our capacities and available resources, we can get to better data to help inform a stronger, more effective anti-trafficking movement.**

Seven Principles of a Data-Driven Movement

1 Human trafficking data can mean many things.

The term "human trafficking data" is an ambiguous concept. When discussing data in the context of human trafficking, there is often an assumption that one is referring either to **prevalence** data or monitoring and evaluation (M&E) data related to donor/government reporting requirements, typically as the sum of cases or programme beneficiaries.

As it happens, existing global human trafficking prevalence estimates are just that – estimates. Though rooted in real, hard data, such as reported trafficking cases or semi-randomised household surveys, these numbers are limited by the impossibility of identifying and reaching significant portions of the trafficked population. In other words, substantial parts of the population we aim to count never had a chance of being included in the observed sample that serves as at the backbone of the given estimate.

In regard to M&E data, it may be the case that

prevalence:

a term borrowed from the field of medicine to mean a proportion of the population affected by a given condition at an exact point in time (stock) or over a specified time period (flow); prevalence is typically estimated based on a sample as opposed to calculated from the entire population

Data should not just be tabulated once a year to produce a report for a government, donor, or multilateral agency; good data collection requires ongoing dedication.

the metrics are largely set by external actors and not strongly linked to your organisational mission or grounded in the reality of your daily operating environment.

That is not to undermine the importance of these two forms of data, but there is other highly valuable information we are missing. There are endless varieties of human trafficking data. For example, direct service data cover the needs of the clients and the services received. Supply chain data give insights into specific industries, commodities, and suppliers. Law enforcement and others rely on tactical data to understand individual human trafficking cases. Anti-trafficking entities can use institutional data to understand how to operate most effectively and maximise the skills of each team member. **Data are not just the number of clients served or the number of prosecutions in a given district – they are also information about people's needs, how they were and will be served, what makes someone vulnerable to trafficking in the first place, what is the *modus operandi* of the crime, what makes a community resilient, what is an appropriate amount of restitution for trafficking survivors, what is a fair sentencing for a trafficker, what encourages policymakers to support anti-trafficking legislation, how do we deter the crime in the first place.**

Data should not just be tabulated once a year to produce a report for a government, donor, or multilateral agency; good data collection requires ongoing dedication.

2 Not all data are created equal.

The private sector has long acknowledged the value of data in informing how to best deliver goods and services that respond to customer demands. The anti-trafficking community, both within government and civil society, is ripe to learn from this experience. But before we can analyse data effectively to **design better interventions and assess our approach and impact**, we must first guarantee that the data we are evaluating is accurate and robust, meaning it paints a full, honest picture of what is actually happening. This is not an easy task, and will no doubt require looking at multiple, diverse sources of data. Moreover, we need to ensure data are collected and used responsibly, placing the needs of those we aim to serve at the centre and prioritizing safety and privacy.

Below are the qualities of **good, responsible data**. It can be challenging to generate data that meet all of these qualifications, but these are the qualities toward which we should all be aiming. Those who are on the front lines of the movement toward better data will no doubt see the benefits in both reputation and allocation of resources.

Good, responsible data are

valid

the data must measure what they purport to measure

For example, a given man's birthdate is a valid reflection of his age; counting his wrinkles is not.

accurate

data should truthfully reflect what they aim to describe

Accuracy requires data to be entered carefully and correctly.

relevant

only information that is applicable and necessary should be collected

For example, we should not collect data on someone's medical history if that information is not central to their case or important in determining services or designing future interventions.

reliable

data fields are clearly defined, lending consistency and fidelity to the information

To achieve reliable data, anyone collecting data within an organisation should be trained to ensure the same approaches, methods, and definitions are used across the board.

impartial

data should be collected in a way that is objective and transparent in its methods while acknowledging and limiting any biases

For example, bias can be introduced by conducting a survey in a given district because it is easy to get to (chances are that area has qualities that make it unique to others) or in the way questions are worded or the language used to conduct the survey (someone might not understand a word in the way you intended or their ability to reply fully might be limited based on the language used).

accessible

data and information on how it was generated should be easily available to key stakeholders both within and outside an organisation

Accessibility refers not only to making data easy to find, but also ensuring it is in a language and format that are understandable and easily available to the user.

timely
the usefulness and validity of data may change over time so it's best to process it quickly for good decision making; real-time data can be incredibly valuable in emergent situations and can also build over time to help us understand trends
For example, information on global migration trends from 10 years ago may not longer be reflective of current patterns.

responsible
there is a duty to ensure people's rights to privacy and security of their information with regard to collection, analysis, storage, presentation, and reuse of data, though whenever possible we should strive for data transparency and openness

empowering
promotes stakeholders having access to the necessary tools, context, knowledge, and skills to make use of the data to meet specific objectives

3 You are a central character in your organisation's data story.

From the community leader to the police officer to the social worker to the journalist to the academic researcher to the NGO director, each and every one of us has a critical role to play in using data to combat human trafficking. Unfortunately, both anti-trafficking NGOs and relevant government agencies working on this issue are often resource-strapped, both in terms of financing and human capital. Many of us are doing jobs that we were not necessarily trained to do or we might not be given adequate tools to do them well. That is not likely to change immediately, but being data-driven ensures our limited resources are used more efficiently and effectively.

Although the task of collecting and recording data is time-consuming and may feel less important than face-to-face client work, the information that good data can support is critical to understanding the nature of human trafficking, and reaching and supporting victims we have not yet identified. Without guaranteed, sustained access to technical expertise to inform our data policies, each of

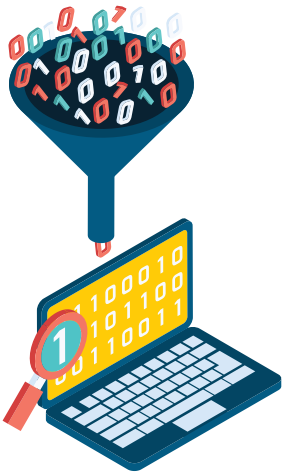
us must develop a basic level of knowledge on these issues and a willingness to implement better policies, even if it initially feels like an uphill battle. On a personal level, these skills will no doubt pay off in advancing your career and should be highlighted on your resume.

Often, what is needed just as much as technical data skills is **attention to detail** combined with **thoughtfulness** and **passion**. Fortunately, these qualities already define much of the anti-trafficking movement.

Asymmetry in access to and understanding of data will only serve to exacerbate existing inequalities. Actors at all levels within the anti-trafficking community, from frontline workers to donors, need to make efforts to **standardise opportunity, resources, and capacity around data**. This guide aims to be a starting place.

We must each recognise the power and responsibility at the core of our work as advocates, public servants, and researchers in shaping and directing the message that reaches policymakers, donors, and other influential actors in the movement to end human trafficking.

Although the task of collecting and recording data is time-consuming and may feel less important than face-to-face client work, the information that good data can support is critical to understanding the nature of human trafficking, and reaching and supporting victims we have not yet identified.



4 Be a critical creator and consumer of data.

Data are as abundant as the conversations about them. From big data to open data to machine learning, the international community talks increasingly about the importance of data in our world. These concepts can be both exciting and intimidating, but just like any other skill, one must start with a solid foundation of key concepts and core practices before moving on to more complex analysis. We must also bring a sense of humility and curiosity to gain a more robust understanding of a complex problem.

It is important to remember that data are not magical. At best they are an accurate reflection

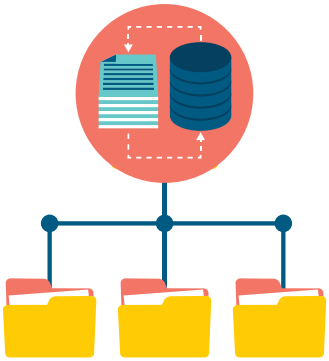
raw data:

data that have not been substantively processed, edited, cleaned, or aggregated

of reality, but at the worst they can mislead us into believing falsities. **Data enable us to systematically track, compare, evaluate, and package what we do, but those outcomes are only as good as the raw data behind them.** Just because information is presented as a compelling statistic or visualised in a striking graph does not mean it is reliable or accurate. It is important that we not only strive to present good data, but that we also become better informed consumers of data. It is useful to consider such questions as the **source of the data** (what is their expertise and authority), any **potential biases of the presenter** (or even your biases as a data consumer), and the **context in which the data should be properly situated**. Moreover, the golden rule of statistics bears repeating: **correlation is not causation**, meaning just because two phenomena occur together, it does not mean one is causing the other.

data set:

a collection of several elements of related information drawn from one or more sources



5 Data should be seen as an asset, not a burden.

Because data are often associated with reporting responsibilities, whether to a donor or a higher level in the government, they can often feel like a burden. But the truth is data have the potential to be extremely valuable in telling us if our work is effective, and how we can do it better.

Many of us may have access to rich **data sets** that are not being fully utilised to shape our work because our limited time is being spent on other urgent tasks. This is like having a treasure chest that you cannot open. If members of your team never have the chance to realise the value of careful data collection

and entry, it is bound to feel tedious. But if that value can be unlocked, it is sure to draw interest and encourage better practices.

Whether we're serving survivors, prosecuting traffickers, or supporting resilient communities, data not only help us impact people's lives for the better, they also make it easier to demonstrate the impact of our work to our superiors and other stakeholders. On the contrary, poor handling and analysis of data can lead to further harm, whether that's compromising the safety of a client through poor data security or getting the facts wrong because of inaccurate data entry. For example, if we see many cases of exploitation coming from a specific province or village, it might seem reasonable to think this is a hot spot for labour trafficking. But perhaps this is a community that is in fact more vigilant about identifying the crime and we've now neglected to invest in awareness-raising programmes in communities that need them more by focusing our attention elsewhere.

When it feels like we're all competing for support and relevance, some anti-trafficking practitioners are hesitant to share their data or even closely scrutinise it internally for fear of learning their programmes are not serving the intended communities well. **But this problem is too urgent for us to waste time repeating past mistakes or not learning from shortcomings; as such, it is critical we learn from and share information on not only what works, but also what does not.**

On the contrary, poor handling and analysis of data can lead to further harm, whether that's compromising the safety of a client through poor data security or getting the facts wrong because of inaccurate data entry.

Transparency paired with a genuine dedication to learning and improvement should be praised – and rewarded – by donors and other stakeholders. And those who demonstrate these qualities early on are very likely to garner more attention and funding. It is true that good, responsible data can be costly in terms of time, money, and human resources (these guidelines contain plenty of low-cost strategies), but the cost of doing this poorly can be people's livelihoods. As donors and governments become more focused on data, setting high standards for yourself will no doubt put you in a good position to attract additional resources.

6 Digital data bring meaningful opportunities, but also challenges.

Digital data can be easier to collect, store, transfer, and analyse, as they do not take up physical space in the same way as paper files. Increasingly, we can employ emerging technologies to aid in and speed up the process, from simply aggregating many human trafficking cases to looking for flows that can quickly be graphed onto a map to more complex tasks of tracing raw materials in a finished product back to factories known to use forced labour. Instead of digging through paper files for the information we need, digital databases allow us to pull up this information instantly through automated search processes, which can save hours of time required in donor reporting, for example. Also, well-designed data systems allow us to update information only once to have it apply to all records for a given case or client. Also, digital data are in many ways more secure if adequately protected because we can easily track who had access to a given record and when.

But digital data also present real challenges in terms of security and effective management. Thinking about water in its various forms is a helpful way of understanding the complexities of securing digital data*. Traditionally our data systems have been built around working with familiar, easy-to-contain forms; think of ice and liquid. Yet digital data are like steam: nearly impossible to control, particularly with outdated systems. For example, if information on a specific human trafficking case was written on one form that was secured in a locked file cabinet to be accessed only by a given set of people, securing and destroying that information is a relatively straightforward process. Whereas case information that has been texted on a WhatsApp chat group can be easily forwarded and shared in ways the source cannot control or necessarily be aware of, and once others have seen it, we cannot undo how it will affect their perception of things moving forward.

It is increasingly important for anti-trafficking organisations to **set organisational policies that proactively address these challenges** to ensure effective data management and compliance with ethical and security standards in the long term (as well as legal standards, which vary by locality). **All in all, the benefits of working with digital data are massive and outweigh the potential challenges if adequately addressed.**

* Credit to Lucy Bernholz of Stanford University's Digital Civil Society Lab.

7 Collaboration is key, but it requires trust and care.

In an environment where resources are limited and people are often working beyond their limits, it is all the more important that we share information and insights in order to **minimise duplicative efforts and maximise collective impact**. If we are ever to have a better understanding of the problem of human trafficking, **collaboration is not an option but a necessity**.

The more we can align our practices, definitions, and standards around data collection, security, and analysis, the movement overall will begin to have more accurate, valid, and useful information driving its work (see interoperability on page 51). From there, we better understand which interventions are working.

Genuine collaboration will also help the movement streamline its objectives, better identify knowledge gaps, and enhance transparency and accountability, including to those communities we aim to serve. Not to mention, we can save tremendous amounts of time by learning best practices from colleagues and replicating or building on them in new contexts. Collaborations must be entered into deliberately and thoughtfully; to be effective, they require dedication on behalf of all members and considerable time. **It is important that partnerships be formalised through regular convenings or other opportunities for cooperation, as well as through protocols, such as written agreements and MOUs. Legally binding contracts will be needed in cases where partnerships involve the exchange of confidential data.**

The more we can align our practices, definitions, and standards around data collection, security, and analysis, the movement overall will begin to have more accurate, valid, and useful information driving its work.

Across the region, there are numerous examples of productive collaboration in the fight against human trafficking, whether cross-ministerial government task forces, NGO coalitions focused on maximizing and sharing resources such as Freedom Collaborative, or **national referral mechanisms**. Everyone has their own specialty in terms of the knowledge and skills they bring to their work; thus, partnering with others can bring valuable new perspectives and information to that work. For example, IT professionals can help ensure we have strong information systems. Medical clinicians help integrate trauma-informed practices into our work. Legal professionals ensure we are complying with local laws. Communications specialists can help ensure our messages are well crafted and reach the right audiences. Not to mention, cross-border collaboration will be essential in this field. **It is rare that one organisation will have all the human resources to address the complex needs of the anti-trafficking field; collaborating is a good way to ensure a more robust approach to our work**. The critical piece for successful collaboration will always be trust. When developing new partnerships or even bringing in volunteers or contractors, it is critical that we verify all actors follow the principles of good, responsible data.

National Referral Mechanism (NRM):

a network of governmental and non-governmental actors working together to identify and support victims of human trafficking

Glossary of Key Terms

ACTIP:
ASEAN Convention Against Trafficking in Persons, Especially Women and Children

anti-trafficking movement:
a group of people with diverse skills and experience in advocacy, social work, research, activism, medical support, criminal investigation, fundraising, legal support, media outreach, and other fields working with the shared purpose of ending human trafficking and supporting survivors

average or **mean**:
the sum of all the observations divided by the number of observations

bias:
a preconceived notion or tendency about a given phenomenon; the introduction (often inadvertently) of an error into the process of data collection or analysis, which leads to faulty conclusions; a systematic overstatement or understatement of the true value of a measurement

biometrics:
information on a person's physical attributes – such as fingerprints, retina scans, and voice recognition – that is often used to verify their unique identity

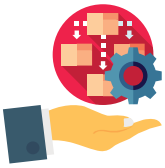
central tendency:
the typical or central value for a given quantitative indicator

cloud/cloud computing:
the internet or other shared network where information, applications, tools, or resources are stored on physical servers in multiple locations and available to access from anywhere; cloud services may be free or paid

cookies: small bits of information about the websites you are visiting sent from your web server (what connects you to the internet) to your web browser (the portal you use to access the internet, such as Chrome, Firefox, Safari, Explorer)

data archiving:
the process of preserving data for easy reference and use

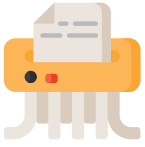
data breach:
the release of confidential data into an untrusted or insecure environment, whether on purpose or by accident



data custodian:
someone with administrative access to and control over data

data de-identification:
the process by which you prevent a person's identity from being connected to data

data dictionary:
a collection of information setting standard definitions and describing the contents of a database and how elements relate to one another in an effort to ensure consistency and proper data management



data disposal:
the process by which data is destroyed securely and responsibly

data field:
a place where you enter data, often a cell in a spreadsheet of a line on a form

data lifecycle:
the flow of data from designing systems to collection to storage to processing to deletion, and everything in between

data minimization:
limiting the personal data you collect to reflect what is relevant and necessary to achieve your objectives and setting procedures for disposing of data when it is no longer necessary

data point:
an identifiable element in a data set; a discrete piece of information

data provenance:
the process of tracing and recording the origins of data and their movement between systems

data retention:
the maintenance of data, ideally for a specified period of time

data set:
a collection of several elements of related information drawn from one or more sources

data subject:
the person whose information is contained with the data; the person whom the data describe

data system:
a way of organizing, both physically and mentally, the processes for data collection

descriptive statistics:
data analysis that describes, demonstrates, or summarises data in a way that allows understanding of trends and patterns

encryption:
the process of converting readable text (plain text) into data that cannot be read without a key (cipher text); essentially encoding a message so it can be unscrambled and understood only by authorised individuals

end-to-end encryption:
communication that ensures only those you are directly communicating with can read the messages; information is hidden even from the provider of the service

gaps:
where are there holes in our data and what do those missing pieces reveal

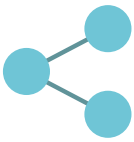
good data: data that are valid, accurate, relevant, reliable, impartial, accessible, timely, responsible, and empowering

harm:
injury to a person, which may be psychological, physical, social, or reputational

human trafficking:
Definition of "trafficking in persons" from the Palermo Protocol: "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs."

inferential statistics:
data analysis that makes informed guesses about an entire population using data drawn from a sample of that population

Internet of things (IOT):
the network of physical devices, appliances, and other electronic items embedded with connectivity mechanisms that enable these objects to exchange data



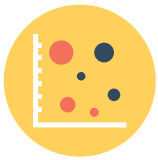
interoperability:
the ability of systems to communicate with one another and share data in a way that makes it accessible and understood

median:
the middle point if all the observations are ordered numerically from smallest to largest (or the average of the two middle points for a dataset with an even number of observations)

metadata:
data that describe or define other data

national referral mechanism (NRM):
a network of governmental and non-governmental actors working together to identify and support victims of human trafficking

open source:
software for which the source code is freely available to the general public for possible modification or redistribution

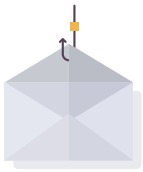


outliers:
data points that clearly do not fit into existing trends or patterns

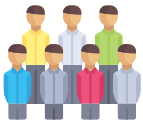
passphrase:
a string of words that is easy to remember, but do not naturally fit together

patterns:
groupings and sequences that arise when comparing people, objects, and events

personal identifying information (PII):
any data that could be used to identify a specific individual; in addition to someone's name, PII can include their passport number, birth date, or address



phishing:
emails that look to be from a trusted source, but in fact come from someone attempting to trick you into sharing private information such as account passwords



population:
the entire group under investigation

positive deviance:
an approach to behavioural and social change based on the observation that in any community there are people whose uncommon, but successful behaviours or strategies enable them to find better solutions to a problem than their peers, despite facing similar challenges and having no additional resources

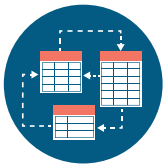
prevalence:
a term borrowed from the field of medicine to mean a proportion of the population affected by a given condition at an exact point in time (stock) or over a specified time period (flow); prevalence is typically estimated based on a sample as opposed to calculated from the entire population

qualitative data:
data typically gathered in a semi- or unstructured manner that describe something

quantitative data:
structured, statistical data that measure something and can be expressed in numbers

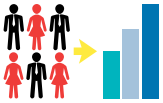
range:
the difference between the largest and smallest value for a given quantitative indicator

rate:
the frequency of a given phenomenon



raw data:
data that have not been substantively processed, edited, cleaned, or aggregated

research design:
the overall approach to the various components of study, from data collection to analysis, laid out in a thoughtful, coherent, and logical way



sample:
the subset of the population that is being observed/whose data are being collected

spread:
the full array of values for a given quantitative indicator

standard deviation:
a specific measure of variation in a given quantitative data set

threats:
data security threats might include employees who lack proper training on security protocols, computer hackers, or out-of-date software/ missing updates for networked devices (such as printers, computers, smart phones, servers, and routers); potential threats to your digital data can come from both within and outside your organisation

trend: a pattern of change or general tendency observed across data points

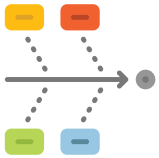
URL:
the address of a website (often starts with www. and is preceded by http: or https:)

value:
the individual designation for each variable, such as male, 32, Chinese

variable:
a specific characteristic of the data subject, such as gender, age, nationality

variance:
a measure of how far a set of observations deviate from the average

vicarious or secondary trauma:
also called compassion fatigue; the negative reactions, including numbness and indifference, that can result from hearing about, reading, or seeing images of someone else's traumatic experiences; second-hand exposure to traumatised populations can create reactions that resemble post-traumatic stress disorder



workflow:
an ordering of tasks or steps towards the completion of a work process, with duties delegated to different people with relevant roles

Data Ethics

The guide begins with a discussion of data ethics because we must ensure that every stage of data collection rests on a strong foundation of **what is right – for each of us, our teams, and those we serve.** Given the personal and sensitive nature of much of the information each of us collects on human trafficking, we must not only be concerned with what we can learn from that information, but how we are protecting the privacy and safety of the people whose data we hold. Data inherently belong to the person they describe; we are only temporary keepers of that information.

NOTE: Civil society organisations in particular must be mindful of the prevailing legal norms governing data collection where they operate, though discussion thereof is outside the scope of this document.

There are numerous ethical issues that arise when working on any human rights issue, and good intentions are not enough to guarantee we are meeting the best interests of those we aim to serve. For example, in an effort to curb exploitation of female migrants, some well-intentioned interventions in the region have inadvertently reinforced the idea that women should stay home, limiting their mobility and agency and likely making them reliant on someone else's care.

From minimizing trauma while collecting information from survivors to building strong data security protocols into your systems, **all ethical data issues rest on the principle of do no harm.** To follow the spirit of this principle, we must give careful consideration to all possible (and likely unintended) impacts of our work on our clients, their families, our partners, staff, and communities. When it comes to combatting human trafficking, it is critical to remember that the primary goal of collecting

Data collection and analysis is a tremendous responsibility. A good starting place when it comes to ethical data is simply a "gut check," meaning would you be comfortable with how things are done if the data in question was about you? This should be supplemented by feedback from survivors and/or data subjects on our systems and approaches.

information in the first place is to better understand the problem so we might fight it more successfully. That means improving the situation of victims and restoring their agency. It means fostering more vigilant and resilient communities. It means getting better at deterring trafficking, and apprehending and prosecuting traffickers.

We must strive to always balance the benefits of data and research against the potential **harm** of unsecured, biased, or incomplete information. Overall, we must always prioritise the safety and security of our constituents, including both our staff and the communities we serve.

Planning ahead and giving consideration to all imaginable outcomes of our work, as well as evaluating our work honestly, including with input from those we serve, are good ways to ensure we are approaching data collection and research ethically. Moreover, this helps us scale successful outcomes and revise those efforts that prove unsuccessful.

The centrality of ethics to all stages of data collection is illustrated throughout these guidelines. For example, we discuss trauma-informed data systems on page 36, informed and active consent on page 34, and proper use of images on page 91. Also, we should give consideration to our team members and ourselves to access opportunities for support given the often difficult nature of the information we are processing and the **vicarious trauma** it may induce.

harm:

injury to a person, which may be psychological, physical, social, or reputational

vicarious or secondary trauma:

also called compassion fatigue; the negative reactions, including numbness and indifference, that can result from hearing about, reading, or seeing images of someone else's traumatic experiences; second-hand exposure to traumatised populations can create reactions that resemble post-traumatic stress disorder

Digital Impact Toolkit has a variety of practical tools to help organisations take stock of their data, evaluate data policies, and implement effective policies around data gathering. https://digitalimpact.io

Ethical data checklist

The following efforts provide a good starting place in integrating ethical data principles more concretely into your organisation's work:

- [ ] Implement a responsible data policy for your organisation that outlines how you will respect the privacy and preserve the security of those you serve while sharing your work in a respectful and responsible manner (see Oxfam **Responsible Program Data Policy in Resources for an example**).
- [ ] Conduct a privacy impact assessment that considers all possible impacts (both purposeful and unintended) of the work on clients, their families, partners, staff, and communities, and outlines a plan to address them prior to beginning any project/programme. This might include:
  - unauthorised use of personal information by authorised parties
  - unauthorised collection, use, or disclosure of personal information to external parties
  - inadequate awareness of the collection, use, and disclosure of personal information of affected individuals
  - unsubstantiated or false identifications of individuals
- [ ] Offer self-care workshops for team members that encourage reflection on what elements of the work lead to feelings of stress, burnout, and compassion fatigue and identify resources and personal practices that offer resilience (see **Trauma and Self Care** in Resources).

Resources:

Updated Guide to Ethics and Human Rights in Anti-Human Trafficking
Issara Institute (2018)
https://docs.wixstatic.com/ugd/5bf36e_1307f698e5ec46b6b2fc7f4391bff4b6.pdf

Guide to Ethics and Human Rights in Counter-Trafficking
United Nations Inter-Agency Project on Human Trafficking Bangkok (2008)
http://www.endvawnow.org/uploads/browser/files/Ethics_Guidelines_Trafficking_UNIAP_2008.pdf

Ethical and Safety Considerations for Interviewing Trafficked Women
World Health Organisation (2003)
http://www.who.int/mip/2003/other_documents/en/Ethical_Safety-GWH.pdf

Guidelines on the Protection of Child Victims of Trafficking
UNICEF (2006)
https://www.unicef.org/protection/Unicef_Victims_Guidelines_en.pdf

Responsible Program Data Policy
Oxfam (2015)
https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950

Trauma and Self Care (from the Manual on Human Rights Monitoring)
Office of the UN High Commissioner for Human Rights (2011)
http://www.ohchr.org/Documents/Publications/Chapter12-MHRM.pdf

Toolkit for Building Survivor-Informed Organisations
Department of Health and Human Services, Administration for Children and Families, Office in Trafficking in Persons (2018)
https://www.acf.hhs.gov/sites/default/files/otip/toolkit_for_building_survivor_informed_organisations.pdf

Istanbul Protocol Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
(Section on re-traumatization of victims)
Office of the UN High Commissioner for Human Rights (2004)
http://www.ohchr.org/Documents/Publications/training8Rev1en.pdf

Digital Impact Toolkit
https://digitalimpact.io

Data Systems

A **data system** is simply a way of organizing, both physically and mentally, the processes for data collection. This includes how we manage data and projects, store data, analyse data, and communicate with your team. Paper intake forms, database software like Microsoft Excel, organisational policies, listservs, web-based customer relationship management systems like Salesforce, and even these very guidelines are all part of data systems.

Any well-functioning data system requires an honest commitment across the organisation to putting good, responsible data at the centre of its design and implementation. Setting up or refining your data system is a fundamental step to ensuring the anti-trafficking movement has better information to shape its interventions and policies. Every ministry, every NGO, every researcher, every journalist, every policymaker has a critical role to play; we are all collecting and disseminating data.

Inconsistency is the enemy of good, responsible data. Fortunately, having systems in place can help reduce these discrepancies. The effectiveness of any data system relies on the practices of its users. That means each of us must agree on and adopt similar definitions and standards of quality.

Systems ensure that we have a way of evaluating our work and meeting the needs of those we serve, while also providing a way for us to track our efforts. This makes it easier for managers to follow the progress of their team as well as for each of us to compile necessary reports about our work. By recording information on paper or digitally (in other words, not just keeping it inside our brains), we can ensure that the work of our organisation will continue even after we as individuals move on to new things.

Setting up or refining your data system is a fundamental step to ensuring the anti-trafficking movement has better information to shape its interventions and policies.

Chances are, your organisation is already generating vast amounts of data on paper forms, in electronic spreadsheets, text messages, emails, and through day-to-day conversation. Considering these diverse and numerous

As a movement, to get the maximum benefit from our data, it is imperative that our data systems are designed around common standards and definitions.

sources of information, it's also highly likely that we do not have the time, training, or systems to appropriately capture all of this data and make proper use of it. But we have the power to change that by constructing thoughtful, user-friendly systems for collecting and analysing data. The key is to have ways to easily record and access data so we can track individual people, cases, campaigns, and programmes over time, as well as understand general patterns and trends.

As a movement, to get the maximum benefit from our data, it is imperative that our data systems are designed around common standards and definitions. This includes a shared understanding of the crime of human trafficking, centred on the definition of trafficking in persons set forth in Article 3, paragraph (a) of the Palermo Protocol (see glossary for full definition), which has been incorporated into most national laws in Southeast Asia. From there, we can set common standards for victim identification and minimum standards of care*. Some countries in Southeast Asia have already implemented victim identification standards used across government and civil society, which is a very promising start! Knowing that our data is collected based on common standards and indicators makes it much easier to compare and analyse collectively.

Strong data systems are also critical to ensuring that data collected at their source, for example at a border crossing, a provincial government office, or over an emergency hotline, move to a central hub where they can be secured and combined with or understood in the context of other information. Data systems might include software that allows us to analyse digital data to create reports based on trends. Data systems can also give us valuable feedback on how our programmes are working (or not) so we can scale up the good components and revise the faulty ones. And of course, digital

*Significant efforts are being made toward these goals, including Common Indicators of Trafficking and Associated Forms of Exploitation developed jointly by ASEAN Member States and Coordinated Mekong Ministerial Initiative Against Trafficking (COMMIT) countries, with support from several bi- and multilateral agencies. The ASEAN Commission on the Promotion and Protection of the Rights of Women and Children is also soon to publish Regional Guidelines and Procedures to Address the Needs of Victims of Trafficking in Persons.

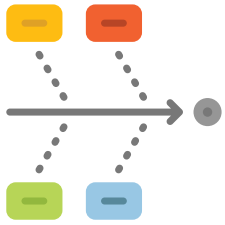
data systems can be used to quickly and easily generate M&E or other required reports on our work.

In order to work well, data systems should have clearly defined **workflows**, meaning how do tasks build on one another to achieve the desired outcome and who is responsible for each step in the process. Defining the "who" for each task should be based primarily on a person's role within the organisation as opposed to simply being random or personality driven as to ensure longevity beyond any one person's time with the organisation.

The main takeaway is that data systems must be, in fact, systematic, meaning they are thoughtfully conceived, reliable, and methodical. With a problem as vast and complex as human trafficking, we cannot afford to do things haphazardly. This section on systems is the longest and most detailed because it serves as the backbone for all of our work with data.

workflow:

an ordering of tasks or steps towards the completion of a work process, with duties delegated to different people with relevant roles



The main takeaway is that data systems must be, in fact, systematic, meaning they are thoughtfully conceived, reliable, and methodical.

Data systems can often accomplish multiple, diverse tasks if they are designed well, ensuring they meet the needs of various actors within a given institution, from frontline workers to office staff to executive directors and government ministers. **Putting effort in at the beginning to understand the environment in which you're operating, including investigating your previous successes and failures (and those of your partners), while being honest about available time and resources, will ensure that the systems you build function practically – and sustainably.** In other words, neither the data themselves nor the technologies we may use to understand and communicate them are enough; we must ensure these systems are designed to meet the needs and capabilities of their users – all of us! Though not ideal in terms of generating large quantities of data for complex analysis, this may mean continuing to operate using pen and paper until you are confident you can adequately secure digital systems. Furthermore, we must never opt for systems or strategies that cut corners at the expense of those we serve. Resources are limited in the anti-trafficking field and not everybody needs or has the capacity for complex, technologically advanced data systems. But as we move toward the goal of good data, understanding how data systems work can help us put practices in place to support future development of more advanced systems.

Start with the questions, not the answers

As anti-trafficking practitioners, the first step to ensuring the principles of good, responsible data are respected is to **raise the question of data from the very beginning – and to consider it at every step of the way in designing and adapting the systems that you use**. Furthermore, we must ensure buy-in from your team; data are only as strong, reliable, and secure as the weakest link among us.

Building data systems is much more complex than developing a digital database; we must first assess what questions we want our data to answer.

Building data systems is much more complex than developing a digital database; we must first assess what questions we want our data to answer. As noted in Data Principle #1, the diversity of human trafficking data makes it challenging to recommend a single, defined approach to designing data systems. That said, there are some basic techniques that apply across the board and can get us all closer to good, responsible data. **The first critical step is to take a high-level view of your organisation's mission to understand what information your team feels is critical to meeting those objectives**. For example, if you are working in the foreign affairs ministry, you might be interested in knowing how migrant workers tend to communicate with their networks back home so you devise ways to reach them with critical information. Or if you're a NGO offering vocational training to trafficking survivors, it is likely useful to know what skills they possess and what their long-term professional goals might be. **The critical point is to not create new objectives based on the data you collect; instead design data systems that are responsive to your organisational objectives.**

Building a database is a tool that helps us get to better outcomes; it is not itself an outcome. Answering the following questions will help you begin to devise organisational systems. Ideally, this process should be done collectively with input from various levels of your team. This will ensure that the vision at the leadership level of the organisation is aligned with the understanding and capacities of those performing day-to-day tasks, including data entry.

Technical assistance in this area can be valuable if your organisation has the resources to contract someone, though it is critical that any outside expertise is balanced with a high level of consultation within the organisation to ensure the system will be adopted and maintained over time.

- What data do we need to collect to do our work effectively?*
- What resources, both human and technological, does your organisation have to facilitate the collection of this information? What skills, capacities, and/or resources are you lacking? Are there potential partners who can support these needs?
- What can we learn from what partners have implemented? What existing systems might we able to adopt and customise?
- Where does data fit in to your organisational objectives?
- How do we build systems that are inclusive and responsive to the needs and desires of those we aim to serve?
- What do you hope your data can tell you? In other words, what questions do you have that you think data could answer?
- What questions do you need to answer to evaluate success in meeting your organisation's objectives?
- Do you need additional data beyond your dataset to answer these questions? If so, how could you obtain these data?
- How do we design systems that minimise bias ?
  Remember, everything from the wording of a question to who asks it to the medium we use to capture it can inject bias into the data collection process. This is unavoidable, but we must endeavour to minimise its effects.

* Use the framework of who, what, where, when, why, but remember to follow the principle of collecting the minimum necessary information. Holding on to non-essential data is only a liability. Additional **data fields** can be added later, though it is best to be as thorough as possible from the beginning to allow for greater comparability across records and over time.

data field:

a place where you enter data, often a cell in a spreadsheet of a field in form

Define the elements of your data systems

Once you have a clear idea of the information you need to perform your duties most effectively and best serve your intended constituencies, the next step is to build or update the systems that allow you to gather and examine the underlying data. Again, acknowledging that every organisation has unique needs and capacities, here is a list of useful points to consider among your team when designing and building data systems. Of course, many times data are being collected in emergent situations, meaning practitioners will need flexibility on protocols to ensure the work remains responsive to potential trauma. That said, having familiarity with and comfort using good systems will support the gathering of more robust data in less controlled environments. Many of these points are covered in more detail in the section on creating a Data Management Plan on page 56.

How will you collect data? In what format(s) is it most useful to you?
This could be a survey, an intake form, a mobile app, an in-person interview, etc. ***What's most important is that the process is standardised as to ensure everyone in your organisation is collecting the same information in the same way****. You should consider how to get the information into a format that makes it easy to process and analyse (for example, transcribing interviews into digital text or entering quantitative data into a .csv file).*

When selecting a format and method for data collection, how do we best guarantee that results are accurate and replicable?
Some suggestions are having clear definitions for key terms and asking the questions in the same way each time.

Is the way we frame questions and define data fields allowing us to get the information we need to know?

How will existing data be assessed for quality and eventually integrated into the new/updated system?

What steps are we taking to minimise errors at the point of data entry?
For example, when recording a date, we define that day comes before month. When a given question/data field has a limited number of possible answers, consider using tick boxes or drop down lists. Also, data should be periodically cleaned to look for data entry errors. For example, if someone's age is listed as 200, we might question it and realise it was entered incorrectly.

Informed and active consent

As you begin to implement data systems, it is critical you have a clear policy on informed and active consent in place. **It is not only important for an individual to know the processes and possible consequences of any kind of service they may accept from your organisation; they must also understand**

the myriad ways their personal data could be used both now and in the future. This requires an understanding on behalf of your team of the full significance of collecting and analysing such personal information, including how the process may be governed by local law.

Whether in law enforcement or social services, anti-trafficking practitioners are often working in environments of uneven power dynamics, making it difficult to secure legitimate consent. For example, can consent be freely given in a situation in which someone is receiving emergency assistance? The more we ensure the spirit of consent is implemented (as opposed to approaching it as the simple tick of a box), the closer we're moving to true consent.

The more we ensure the spirit of consent is implemented (as opposed to approaching it as the simple tick of a box), the closer we're moving to true consent.

As we increasingly work with digital data, which are easily duplicated, re-purposed, and disseminated, we must acknowledge that the ways we use information and the intended outcomes of their use may be continually in flux. Furthermore, as we know, legal processes and social services are often taking place on long timelines so these questions need to be revisited and revised continually. Those controlling the personal data of any individual should be sensitive to this fact and seek additional consent as the purpose changes from the time consent was given.

Consider using the consent process as an appropriate opportunity to start a dialogue amongst both your team members and those you serve on the impacts of online or digital identity, essentially the collection of all fragments of information related to who we are that are widely dispersed online. Every action we take while networked – from what we post on social media, to what websites we visit, to any webforms we fill out – leaves a digital trail linked to our identity and will likely become increasingly difficult to secure. It is especially important that this concept is understood if people's personal stories and/or images will be shared online as part of your programmes.

It is useful to consider the following **key elements of informed and active consent** when designing consent procedures for your organisation, ideally with input from survivors:

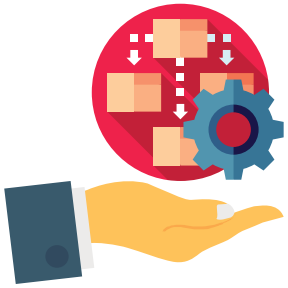
- The identity of the data collector and the organisation they represent should be clearly stated
- A narrow, specific purpose of data collection as well as how it will be secured, communicated, and potentially shared should be made clear, as well as the associated potential benefits and risks
- Clarity on which components of the data may be used, and if the individual's identity is meant to remain confidential
- Written or recorded certifications of consent should be kept on file alongside the relevant data
- Consideration for how long the data may be used and in what formats
- A process for subjects to request their personal data or withdraw consent should be clearly outlined and contact information for the **data custodian** shared (and updated as needed)
- Consent must be given freely and voluntarily, recognizing inherent power dynamics that shape this process (staff should be appropriately trained on signs of distress to ensure consent is valid)
- All of this must be communicated in a format and language understood by the data subject, who must not be incapacitated at the time of consent
- Consent should not imply the waiving of rights or release from liability due to negligence on behalf of the data custodian/the organisation they represent
- If cash or non-monetary compensation will be offered, it is important that the interviewee is genuinely interested in participating (as opposed to being drawn by the promise of compensation, which can arguably be a form of coercion)

Secure and trauma-informed data systems

As emphasised in the earlier section on ethical data collection, for those of us working with potential trafficking survivors, every aspect of our work must integrate robust security protocols and an awareness of the pervasive nature of trauma among this population. Security protocols are addressed in detail in the section on Data Security (pages 61 – 71) so here

data custodian:

someone with administrative access to and control over data



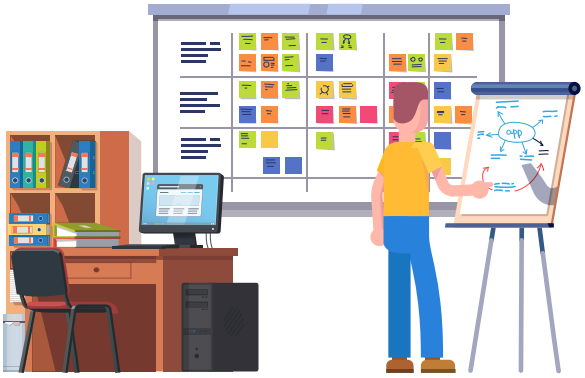
we will focus on creating systems that account for the high incidence of trauma among human trafficking survivors.

An important starting place is educating our staff about the nature of trauma and its effects. This has the added benefit of ensuring our teams are aware of the impacts of secondary trauma, as mentioned on page 26. From there, we can ensure a safe, comfortable environment that also provides opportunities for survivors to be empowered and regain a sense of control and agency. If we acknowledge the tremendous value of data, it is easy to understand that data collection can create a power imbalance between the data subject and those collecting the information. This fact should be kept in mind as we approach gathering information in a way that encourages empowerment for trafficking survivors and avoids re/traumatization.

To ensure we are setting up data systems that take these dynamics into account, we should follow these principles:

- Build trust and confidence with data subjects while ensuring the accuracy of data collected
- Do not rush the interview/survey process so as to allow clients to feel understood and supported
- Emphasise the value of the information collected in informing higher quality services both among your team and when interacting with data subjects
- As much as possible, conduct meetings in a private, quiet, secure, and comfortable space in which the client has some level of control to choose the seating arrangement, take breaks, or get water/a snack, for example

If we acknowledge the tremendous value of data, it is easy to understand that data collection can create a power imbalance between the data subject and those collecting the information.



- Develop and share standard instructions for interviews with your team to ensure consistency, completeness, and accuracy, thus enhancing data quality
- Have psychological and psychosocial support on hand before, during, and after interviews whenever possible
- Give special consideration to the value and responsibility of professional interpreters and awareness of cultural differences in data collection

Integrate diverse expertise into system design

A general challenge in the human rights community broadly that is certainly relevant to any conversation on human trafficking data is the challenge of communicating effectively between the wide range of actors involved, from frontline human rights defenders to technical experts to policymakers. Because we generally work within rather isolated frameworks informed by our unique experience and perspective, it can be challenging to create systems that successfully incorporate all parties' unique expertise in both meeting the technical demands around data collection and security while also responding to the capacities and needs of the team.

It is rare that someone possesses both the skills to build technically complex data systems and also respond to human rights crises, but we can all make a better effort to appreciate and learn from one another. **A first step for this is to start speaking the same language, literally and figuratively, and try to avoid specialized, technical vocabulary**. Instead, explain what these terms mean as you make an effort to understand each other's work. The glossary on page 19 aims to begin breaking down some of these terms.

Take a data inventory

When considering a new or updated database, is it important to first consider the data that you already have, evaluating what you collect against what you actual use in meeting your organisation's objectives and understanding your work. This will ensure we are following a policy of **data minimization**, essentially limiting what you collect and keeping it only as long as you need it. That is not to say you should not explore additional data fields that seem relevant, or could be in the future when designing your data systems, but you should have a valid justification for what you collect. In addition to limiting the potential for **data breaches** and violations of privacy, organisations can save time and money by eliminating unnecessary data collection and not storing data beyond their point of utility. Though damage to the data subject is of paramount concern, organisations must also

data minimization:

limiting the personal data you collect to reflect what is relevant and necessary to achieve your objectives and setting procedures for disposing of data when it is no longer necessary

data breach:

the release of confidential data into an untrusted or insecure environment, whether on purpose or by accident

consider the potential reputational damage of compromised data. It is important to encourage staff to report any issues as soon as possible in the hopes of correcting the situation quickly and learning from the experience to strengthen systems and protection methods. Such incidents should be catalogued in order to identify possible incident patterns.

Victim identification standards

If we as a movement are trying to better understand the qualities and circumstances that make people vulnerable to human trafficking or appropriately characterise those who have been victimised, it must be absolutely clear who is a victim and who is not.

Having clear and well-defined criteria for identifying potential victims of human trafficking is not only critical to ensuring adequate protection and support are provided, but it is also a key element to improving data quality. If we as a movement are trying to better understand the qualities and circumstances that make people vulnerable to human trafficking or appropriately characterise those who have been victimised, it must be absolutely clear who is a victim and who is not.

Of course, not all anti-trafficking entities play a role in identifying or verifying who is a victim, but for those that do, it is important that all members of your team who may come into contact with a potential victim of trafficking be trained on basic victim identification standards. Internal standards must be set on not only the signs and indicators of a potential victim, but also the processes by which they will be identified.

Because victim identification processes must reflect the relevant national legislation defining the crime of human trafficking, it will be difficult to have a unified form and process across Southeast Asia. **But, what can help support comparability of data generated by such assessments is setting out clear standards and protocols – and being willing to share those publicly**. This will support the effort to align principles and practices as much as possible.

Being that victim identification processes must reflect the relevant national legislation defining the crime of human trafficking, it will be difficult to have a unified form and process across Southeast Asia.

Some important considerations when developing identification forms and standards for implementation include:

- Tools should be carefully developed to capture multiple types of potential victims, such as those trafficked internally v. cross-border, or those trafficked for sex v. forced labour
- As much as possible, validate screening tools across multiple fields, such as law enforcement, the judiciary, and social services, to ensure they are relevant and sufficient for the widest possible audience
- Be sensitive to cultural factors around religion, gender, social norms, attitudes towards sex and sexuality, etc. both in development and implementation of such tools
- Test tools before finalization to ensure they are user-friendly and do not take too long to complete
- Special consideration should be given for identifying child victims and protocols/forms will vary
- Once screening tools are validated, ensure staff are properly trained on their use, including on how they present physically and verbally to the client as well as being prepared to handle any trauma that surfaces
- As discussed on page 36, ensure the development and implementation of any screening form is trauma-informed, ideally with input from survivor leaders *Sometimes it is helpful to pose questions indirectly. For example, instead of asking someone directly if they were told to lie about the type of work the engage in, you could instead start with "Sometimes people are forced to lie about their work situation ... has this ever happened to you?"*

It is important to acknowledge the difference between quick, informal checklists and more detailed, formal assessment tools. The former is likely useful in an emergency setting or when decisions about care and safety need to be made quickly. As previously mentioned, the following list of visual cues as possible indicators of a situation of human trafficking was developed specifically for ASEAN and COMMIT countries. This can be considered more of a list of "red flags" that someone is currently or formerly in a situation of trafficking (as opposed to being vulnerable to future trafficking) and their situation should be investigated further.

- Signs of control/surveillance (e.g. fences, cameras, weapons)
- Signs of fear/distress/depression/ psychological abuse
- Demonstrates lack of familiarity with environment/situation
- Inability/unwillingness to communicate (e.g. language barriers, no mobile phone, instructed on what to say)
- Age/status of potential victims (e.g. unaccompanied children, persons appearing to be under minimum legal age for situation/place of work, children in an inappropriate situation)
- Signs of physical abuse, physical damage, poor physical condition
- Working environment appears unusually dangerous with reference to the person's age/condition
- Conditions on the job appear to be very poor (e.g. working very long hours, no breaks, no time off)
- Living conditions appear to be very poor (e.g. food, sleeping arrangements, large numbers living at the place of work)

(See **Identifying Victims of Trafficking and Associated Forms of Exploitation: Common Indicators for First Responders** in Resources)

Of course, a more in-depth and formal assessment would need to be conducted (by a qualified practitioner) for use in a legal case. This would need to track the elements of the crime and ideally collect other relevant information about the potential victim to be used not only in legal proceedings, but also in ensuring safety and providing holistic care. Further down the line, such data can be aggregated in an effort to identify trends and patterns useful to improving detection, service provision, and, ideally, preventative measures.

Define your methods for data collection

No matter the approach to data collection – a random household survey, client intake form, hotline call, or criminal investigation, for example – **we must be aware of the impact our methods have on our results**. For example, open-ended questions will produce different information than those with a limited selection of possible answers; people will respond differently to questions asked in person versus an anonymous mobile phone survey.

Relevant data collection methods might include correlation and association, surveys, regression

analysis, network analysis, case studies, textual analysis, participant observation, longitudinal studies, structured and semi-structured interviews, and focus groups.

As such, we must carefully consider the methods for data collection before beginning intake. As discussed further in Data Presentation and Visualization on pages 89 - 96, when we report data, we should also include relevant information on how it was gathered and analysed to ensure that those consuming the information have an accurate interpretation of what is being presented. A good place to start is with the objective or goal of the research. It is helpful to share questionnaires, blank surveys, forms, or other tools used for data collection along with definitions of any key concepts contained therein. In the case of surveys, it is important to share how representative the sample is of the entire population as well as information on non-responses.

Define your data elements

In the same way a traditional dictionary ensures common understanding of vocabulary, a **data dictionary** names and defines the purpose and scope of key data elements. **This is helpful not only for consistency within an organisation, but will ensure data are properly understood and interpreted when shared with others.**

Given the diverse roles and responsibilities of actors in the anti-trafficking field, different data will be collected by each entity. **Therefore, it is important that we agree on the scope and meaning of common data fields.** Defining terms is not always as easy as it seems. For example, the concept of gender changes over time and across cultures. Establishing definitions will help create cohesion and agreement across your organisation, ensuring the accuracy of the data as well as how others outside the organisation understand it when presented publicly. It could be useful to periodically review fields that consistently present challenges for the team for revision, for example, if you see errors during data entry or understanding of the definition is unclear.

Your data dictionary should always accompany relevant data files/databases. It may be useful

data dictionary:

a collection of information setting standard definitions and describing the contents of a database and how elements relate to one another in an effort to ensure consistency and proper data management

to consult with colleagues at other organisations or across government agencies in an effort to align definitions and fields to allow for greater comparability. The data dictionary for the Counter Trafficking Data Collaborative, a global data hub on human trafficking that hosts de-identified and aggregated case data from the International Organisation for Migration, hotline data from Polaris, and NGO partner data from Liberty Asia, is available at https://tinyurl.com/ctdcdictionary

Key elements of a data dictionary include:

- **Attribute name**: essentially the column header or label for each element of your data

  For example, family name, given name, birth date, date of meeting, gender, place of birth, etc.

- **Definition**: clear statement of what this attribute represents

  For example, if collecting data on a person's physical address, make it clear what information you want (nearest cross streets, name of the village, a street address, a pin on a map, etc.)

- **Type of data**: Description of the data's characteristics, such as if it is text, numeric, a date, an email address, a drop down list, as well as any limitations on entry

  For example, state the allowable number of characters or a list of possible options for tick boxes.

- Field is **required or optional**

  Digital databases can be programmed to require certain fields before a record can be saved.

Classify your data based on risk

Once a data inventory is taken, it is useful to classify your data based on the level of confidentiality it affords and the severity of any adverse consequences that might result from that data being lost or compromised. It may be easiest to think of your data in terms of **high**-, **medium**-, and **low-risk** and then set standards for each classification.

As an example, high-risk data would include personal health information for a trafficking survivor or other personally identifiable data, such as contact information for family members or bank account information. Medium-risk data might include non-public information that your organisation would not want to be shared, such as internal policies or research that is not yet released. Low-risk data is essentially information that is already public, such as what is published on your organisation's website or in printed materials that are widely dispersed.

Different levels of data access, or access control lists, should be considered for each type of data. Those with access to more sensitive information should be adequately trained and demonstrate willingness to take the proper care in protecting that data.

Metadata – data that describe or define other data – can be a very important element of processing information accurately. Metadata can tell you when and where an image was captured or who conducted a given interview and in what circumstances, for example. There are times where we will want to be deliberate about collecting/analysing metadata, such as within the investigation phase of a trafficking case, but we should also be cautious to remove metadata from images when sharing them publicly (or configure devices not to record them in the first place). In the same way metadata are attached to the data they describe, consider also cataloguing any useful information on **data provenance** alongside the files, such as how it was collected or if it has been edited. Metadata should live with the data and be shared when the data files are shared.

data provenance: the process of tracing and recording the origins of data and their movement between systems

Ensure data are clean

Small errors made during the data collection/ entry phase can have large, unintended consequences. For example, misspelling a person's name might mean their record is not matched with a related entry or inputting a **value** incorrectly could distort the average for that data field. Fortunately, there are various techniques that can be employed in the data entry phase in an effort to ensure data cleanliness and quality.

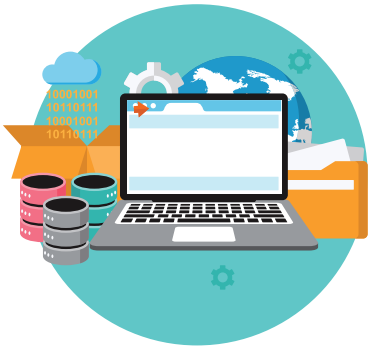
Value:

the individual designation for each variable, such as male, 32, Chinese

- Forms and databases can be set up to ensure required fields are not left blank
- For fields with a limited set of possible responses, tick boxes or dropdown menus may be used

  For example, this is particularly useful for location data so that data can be correctly geo-coded, or translated into geographic coordinates, to display on a map.
- Constraints can be placed on data types at the point of entry in digital systems

  For example, fields can be set up to only accept certain types of data, such as dates, email addresses, or phone numbers.



- Fields that have a set range of values can be constrained by minimums and maximums in digital systems
- Digital databases can be set up to ensure that specific entries are not repeated

  For example, if a name or unique identifier is used (such as a case number or state-issued ID number), it cannot be used in a new, unrelated entry
- Ensure that your team has a protocol for differentiating between an empty cell/ field (missing information), unknown (meaning the value is unknown), N/A (meaning no data available), subject declined to provide information, and 0 (for a zero value)
- Set up a system to easily identify duplicate records, either manually or, ideally, as a function of a digital database system
- Set a regular time to review protocols for data entry to ensure they're working for your team and address any inconsistencies/questions

Resources:

Counter-Trafficking Data Collaborative
https://www.ctdatacollaborative.org/

Identifying Victims of Trafficking and Associated Forms of Exploitation: Common Indicators for First Responders
United Nations Actions for Cooperation Against Trafficking in Persons (2016)
http://un-act.org/publication/view/identifying-victims-trafficking-associated-forms-exploitation-common-indicators-first-responders/

Adult Human Trafficking Screening Tool and Guide
Department of Health and Human Services, Administration for Children and Families, Office in Trafficking in Persons (2018)
https://www.acf.hhs.gov/sites/default/files/otip/adult_human_trafficking_screening_tool_and_guide.pdf

Guidelines for the Collection of Data on Trafficking in Human Beings, Including Comparable Indicators
International Organisation for Migration (2009)
http://publications.iom.int/bookstore/free/guidelines_collection_data_IOMVienna.pdf

Oxfam Responsible Data Policy
Oxfam (2015)
https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950

A Guide to Data Innovation for Development
UN Global Pulse (2016)
http://unglobalpulse.org/sites/default/files/UNGP_BigDataGuide2016_%20Web.pdf

IOM Data Protection Manual
International Organisation for Migration (2010)
http://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf

A World that Counts: Mobilising the Data Revolution for Sustainable Development
United Nations Secretary-General's Independent Expert Advisory Group on a Data Revolution for Sustainable Development (2014)
http://www.undatarevolution.org/wp-content/uploads/2014/11/A-World-That-Counts.pdf

DATANAV: How to Navigate Digital Data for Human Rights Research
The Engine Room, Benetech, Amnesty International (2016)
https://www.theengineroom.org/wp-content/uploads/2017/01/en-datnav-report_lower-quality_web_.pdf

Human Rights and Data: Tools and Resources for Sustainable Development
The Danish Institute for Human Rights (2017)
https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/sdg/data_report_2016.pdf

Professional Standards for Protection Work
ICRC (2013)
https://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf

Databases

As more data become digital, the systems we use to collect, store, and analyse that information will need to be increasingly flexible. **Organisational systems must not only be adaptable to technological advancements, but also changes in the operating environments, such as new laws governing personal data, which are likely to proliferate in the near future.** Furthermore, the utility and value of data changes over time, particularly in the context of emergent human rights violations.

Data points that initially seem essential to providing adequate, individually tailored relief or care, such as personal health information or family contacts, may increasingly pose a risk to the data subject if they are not properly secured and eventually destroyed when no longer needed. Any system can be built to ensure both privacy and safety, and attention must be paid to this careful balance continuously.

Databases, essentially digital filing cabinets, are a key element of your data system. Ideally, a digital database makes many elements of our jobs easier, particularly when it comes to accessing necessary information for understanding and reporting on our work. For example, we can quickly run a query in a digital database to identify if multiple victims are coming from the same geographic area or if the same recruiting agencies are involved

Ideally, a digital database makes many elements of our jobs easier, particularly when it comes to accessing necessary information for understanding and reporting on our work

data points:

an identifiable element in a data set; a discrete piece of information

in trafficking cases. This task is much more complicated if one has to manually compare hundreds, if not thousands of paper files. Ensuring that your team, particularly those in charge, appreciate these potential benefits will help in overcoming the initial investment of significant time and resources in getting such systems up and running (though resources can be saved by doing a careful analysis of what systems partners are using and reviewing out-of-the-box software to see if something that already exists meets your needs).

In many cases, your database will also likely serve as a project management tool; in other words it is not simply a repository, but also a way of tracking your day-to-day operations. Familiar databases may include Microsoft Excel and Access; the Victim Case Management System (VCMS), currently offered free of charge by Liberty Asia with support from Salesforce and the U.S. State Department; and Google Sheets. These collections of data should be organised deliberately to allow for the quick and easy retrieval of information, while also providing a structure for data storage, modification, and deletion. Many web-based systems, such as G Suite (Google and Salesforce) and Airtable, have built-in forms that automatically transfer data entered into a form into the appropriate data fields. Some databases include features to allow for data analysis in addition to mere **data retention**, such as the ability to generate basic statistics or look for trends and outliers (this is covered more in depth in Data Analysis and Interpretation on page 79).

As covered in Data Principle #6, though it is important to address the unique challenges posed by digital data, moving information from paper into digital form provides crucial new opportunities for analysis and learning that are sure to improve your work overall, as long as security remains a top priority.

Ensuring that your team, particularly those in charge, appreciate these potential benefits will help in overcoming the initial investment of significant time and resources in getting such systems up and running

data retention:

the maintenance of data, ideally for a specified period of time

Anytime you are using free or paid software, ensure you are comfortable with the conditions of the Terms of Service, giving particular attention to what information the service provider collects about you as the user and any rights the service provider has in terms of the content you enter into their system. As previously mentioned, there is often a tradeoff between convenience and security, and we must be mindful of this.

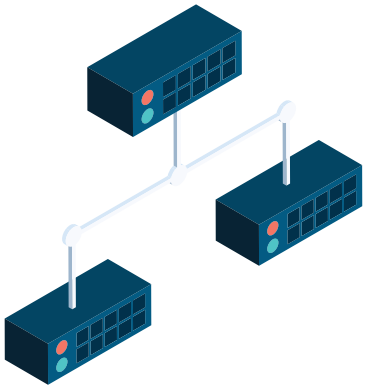
Building a single database that meets the unique needs and specifications of the numerous types of actors in the anti-trafficking community would be extremely challenging, if not impossible. **That said, it will not be critical that we are all on the same exact system, but that we endeavour as much as possible to ensure standardisation and comparability across systems – essentially interoperability**. This means setting standards for good data practices as outlined herein to ensure data from disparate sources can be combined, de-duplicated, and collectively analysed, whether that's trend analysis to establish trafficking routes or understand what makes advocacy campaigns effective, or tracking an individual case across different service providers to ensure survivors' needs are being met holistically. Moreover, working together to design systems that are interoperable and make data sharing easier (in a way that is still sensitive to privacy issues) can help limit the need to re-interview, and thus potentially re-traumatise survivors and other relevant stakeholders.

Though user experience design (often called UX) is important, avoid being lured by systems that are popular, flashy, or novel if they are not also practical – **what's most important is finding or building a system that meets your needs and will be adopted by your team**. Sometimes tools that seem particularly exciting or innovative may be more complicated – and cumbersome – than we actually need.

On a related note, it can be helpful in certain cases to bring in a consultant on technical matters such as setting up new digital data systems. However, remember that no amount of outside expertise can substitute for local knowledge, both of the issue areas you work on as well as the day-to-day operating environment. If considering bringing in outside expertise, ensure whatever systems they help create are sustainable beyond their contract, including any necessary software updates, system upgrades/changes, and long-term access. Also, it is important to be clear that all data ownership remains with your organisation even when contracting an outside service.

interoperability:

the ability of systems to communicate with one another and share data in a way that makes it accessible and understood



In any database, each individual record must be as accurate and complete as possible. From a policy perspective, the utility of data increases as it is combined with or analysed alongside additional data sets, as long as they, too, are of good quality and relevant. This enables us to look for trends and design policies that have the greatest effect on the greatest number in a given industry or location, for example. That said, we must not overlook the value of granular data at the level of the individual so that services can be tailored to a given person's situation, whether this is direct service provision or determining the jurisdiction for a legal case.

Database creation framework

It bears repeating that the most critical element of a database, a central component of any data system, is functionality – does your team find it useable and does it meet your current organisational needs while also making consideration for future development strategies. At a basic level, we use databases to ensure our data are readily available and easy to find when we need them. They should be easy to manage and adequately secured while minimizing redundancy in data storage. As such, when setting out to create a database, move on to a new system, or update your current system, these questions may help guide the process:

- Are the processes of data entry manageable for your team?
- Are data available to your team at any time when and from any location where they might need access?
- Will the speed of the system be manageable with existing equipment and internet service?
- Can the database handle the volume of data you plan to manage?
- If the system is web-based, can it be accessed offline in the case the internet is not functioning?
- If the system is web-based, how often will records be updated and saved?
- Is it easy to make changes or add new fields at a later time?
  Make consideration for differentiating or somehow marking entries that are verified versus those that are approximated, such as when a birthday can be confirmed with official identification or when age is not definitively known.
- Does the database offer adequate security features?
- Does the database easily accommodate different user groups with distinct permission settings (called "access control lists")?
  For example, for organisations with social workers, lawyers, and investigators working on the same cases, can permissions be set to ensure only relevant employees see the appropriate information (such as modus operandi *or medical records).*
- Is access to the database easily granted and revoked as employees change?
- How often and to what location will data be downloaded as a backup or for archival purposes?
- Can data be entered into the same record simultaneously by multiple users?
- Does the system easily catalogue relationships between records?
  For example, can multiple perpetrators be connected to the same case or can social workers in multiple organisations be linked to a client's record? This is often a critical component of functionality for any data system.

- Does the system offer varying types of data entry, such as freeform text, tickboxes, drop-down menus, etc.?
- What features can be integrated to improve the accuracy of geographic data points?
  For example, some systems, including VCMS, enable the user to drop a pin (as you might on a smart phone map application) to identify an important location. Or, can drop down menus be created hierarchically in a way that options change as you drill down, for example from the national to village level?
- Can electronic files (such as document and image files) be attached to records in the database?
  For example, ensure documents related to court proceedings or images of evidence can be uploaded and linked to a given trafficking case.
- Does the process of extracting data from the system meet your needs? Are there built-in operations for data visualisation? Can data be downloaded in appropriate formats, such as .csv files? Can graphs from the dashboard be downloaded in an appropriate format (.png or .pdf)?

These considerations point to the importance of collaboratively designing databases with both substantive experts (you and your team members who are intimately familiar with the work and day-to-day operations) and technical experts (those skilled in computer science and web development who can easily guide you through available technologies and options).

Data Storage

Once we have developed systems that allow us to collect the data we need to best serve our communities in a way that fits our capacities and available resources, we must then consider **how these data will be maintained and managed**. This step is critical to realizing the benefits of the time and resources invested in designing a robust system. Data storage is a critical stage in the **data lifecycle**; we must ensure data are safely and securely stored while remaining accessible to those who need them to evaluate the organisation's day-to-day operations as well as the impact of their work.

data lifecycle:

the flow of data from designing systems to collection to storage to processing to deletion, and everything in between

This section is focused on the maintenance of digital data, though similar considerations should also be made for paper files, such as how and where they will be stored to prevent theft, loss, or damage, and who will have access to what documents (and how this will be regulated). If direct digital data entry is not an option, consider if it makes sense to scan hard copies, knowing that you would likewise need to secure the soft, digital copies.

Develop a data management plan

A data management plan helps ensure proper data maintenance, including providing back-up plans to address common data challenges, while also building a culture of good data practices amongst your team. A data management plan will create a record, and thus accountability, around many of the data practices and principles covered herein. **This document will lay out a strategy for the entirety of the data lifecycle, from systems design to collection to analysis to sharing.** When fleshing out a plan, keep in mind how each component could potentially impact the privacy and security of the data subject, aware that you may need to edit your plan as time goes on and your data needs change.

Here is a list of potential components of a data management plan, again acknowledging that each of us has unique needs and a distinct operating environment.

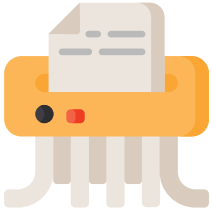
- Consent procedures (see page 34)
- Data inventory including, data types, sources, locations, and formats (see page 38)
- Data uses
- **Data archiving**
- **Data disposal**
  Establish how long will data will be stored, noting that some data privacy laws stipulate a period of time at which data must be destroyed for inactive records. See section on ***Data deletion*** *on page 68 for guidance.*
- Data security (see page 61)
- Inventory of relevant hardware and software and how they're used within your organisation

data archiving:

the process of preserving data for easy reference and use

data disposal:

the process by which data is destroyed securely and responsibly



- Establish brief, but descriptive naming conventions
  Following a standard procedure for naming documents ensures consistency and makes retrieval easier. Using underscores "_" instead of spaces in the file name can help ensure compatibility across different computer systems.
  You may also consider including version history in the name if you've been working in a document over time, inserting "v1" or "vFinal" at the end of the file name.

- Listing of those working with/accessing organisational data and their roles, responsibilities, and permission levels (see page 52)
  Include information on how you will ensure your team knows the data protocols and methods you set out.

- Outline how new staff will be trained on data systems and how organisational data on personal devices will be secured when staff leave

- Internal and external data sharing and disclosure processes (see Data Sharing on page 73)

- For in-person data collection surveys/ interviews, consider if data entry will be done in the presence of respondents or will it be input later
  Consider how data entry will affect the nature of the interaction.

- For those working on case management, establish how often data will be updated for a given individual and how progress will be tracked

- Document the governing policies/ regulations related to data in the places where you work (or where digital data pass through)

- Establish a policy for ensuring data quality, including data cleaning
  If your work includes building legal evidence to be presented in human trafficking cases, careful attention should be paid to building data systems that ensure the integrity of the data and allow for an auditable chain of custody (knowing who had access to the data at all times). Metadata, as discussed previously, can be helpful here.

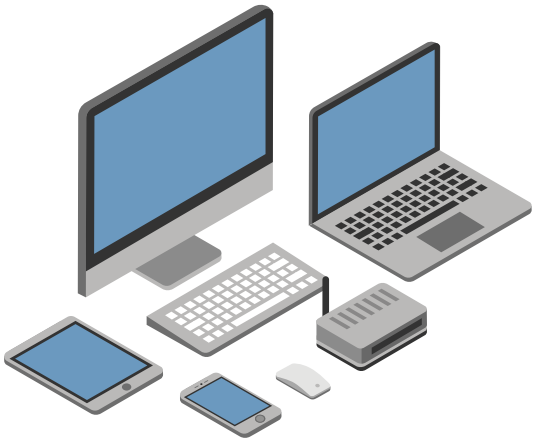
- Establish a backup plan
  If your digital data are stored locally (as opposed to on the cloud where backup is typically automatic), ensure you have a copy stored on a second hard drive in a different location, but with the same security and privacy measures in place. Remember that a backup is essentially a snapshot of a file at a given point in time and does not automatically update with the original file.

- How will data be cleaned/checked for accuracy?
  You might also consider creating mock data sets for data entry and cleaning for your team to practice.

Storage options from computer to the cloud

There are a growing number of options when it comes to storing digital data, each with its unique advantages and disadvantages. We will quickly outline some of those options here so you may weigh which is best suited to your data and operating environment.

Local/personal computer (or other electronic device)



- ⊕ clear control of the data at the individual level, secured from outside access if properly encrypted and securely stored
- ⊖ subject to loss, theft, confiscation, destruction; unable to access from remote locations; no backup

Private network

- ⊕ data are more resilient to loss of any single device while providing clarity of control at the organisational level, easy to collaborate and share with others on the network, frees up hard drive space on devices
- ⊖ challenges to securing data, cost of maintaining the network, potential reliance on outside support to secure and maintain systems, susceptible to data loss if server is compromised

Cloud-based storage

- generally affordable, potential IT support from provider, data are backed up to physical servers in multiple locations so risk of data loss is highly reduced, frees up hard drive space, easy to share/collaborate within and outside the organisation, accessible from multiple locations through log-in
- questions of control over the data may be unclear depending on terms of service, data access controlled by a third party whose policies may fluctuate

If considering cloud-based storage, ask colleagues for recommendations in your area and look for providers who value data protection and privacy, offer reliable and rapid customer support, and are trusted in the anti-trafficking field or human rights more broadly. Moreover, you should negotiate an exit strategy should you wish to terminate your account that includes full retention of your data for your organisation and complete deletion from their servers.

the cloud/cloud computing:

the internet or other shared network where information, applications, tools, or resources are stored on physical servers in multiple locations and available to access from anywhere; cloud services may be free or paid

Data Security

Many of us working in the anti-trafficking field have unique access to very private, possibly sensitive data, including information related to health, family histories, personal behaviours, migration histories, and more. **This is why we must prioritise keeping information secure; from there we can focus on designing systems that help us gather the information we need to do our work effectively.**

Though it is impossible to guarantee security, if a critical level of protection cannot be achieved, alternative avenues for data collection and management must be explored or sensitive data should not be collected in the first place.

Data collection related to human trafficking naturally presents risks to the data subject, their families and personal networks, as well as the person (and their organisation) collecting the information, including potential for physical, psychological, or reputational harm. **Many of us are in this work because we believe strongly in an individual's inherent human rights, which implies a duty to ensuring their safety and protecting their right to privacy.** We can operationalise those norms in our everyday practices by doing things like selecting strong passwords (page 65), encrypting data (page 63), and understanding the myriad risks inherent to being a data custodian. Small changes to our daily practices can have big impact when it comes to protecting confidential data from accidental disclosure and it will be critical that every level of your team is aware of and addresses their vulnerabilities.

The responsibility for protection of sensitive information is a shared one. All personnel in a given organisation should be familiar with relevant organisational policies, as well as local and national laws governing the protection of data. Though it is impossible to guarantee security completely, if a critical level of protection cannot be achieved, alternative avenues for data collection and management must be explored or sensitive data should not be collected in the first place. Civil society organisations in particular must acknowledge that the operating environment is often unregulated where it might be in the private or governmental sectors, thus there is an added responsibility of self-regulating to ensure methods and approaches are secure and that we are accountable to our stakeholders. In the end, it is critical that any security mechanisms we adopt are not overly complicated or difficult to use; we cannot afford to waste valuable resources on mechanisms that will not be adopted in practice.

In the same way that one cannot collect physical objects without a proper container to hold them, we should not be collecting digital data until we have a secure, reliable way to store that information. **By their nature, digital data move easily, making it at times challenging to track them and safeguard them from unauthorised access.** In the same way we would lock a file cabinet containing sensitive records, we need to find ways to protect digital files from unauthorised access. As more and more electronic devices come with the ability to connect to a network (consider the **Internet of things**), we must remember it is not only our computers that need securing, but also our smart phones, tablets, data storage devices such as external hard drives and USB devices, digital cameras, and printers or copy machines.

Internet of things (IOT):

the network of physical devices, appliances, and other electronic items embedded with connectivity mechanisms that enable these objects to exchange data

threats:

data security threats might include employees who lack proper training on security protocols, computer hackers, or out-of-date software/ missing updates for networked devices (such as printers, computers, smart phones, servers, and routers); potential threats to your digital data can come from both within and outside your organisation

After reviewing these guidelines on data security, it would be useful to conduct an assessment of your organisation's current practices around security, giving particular attention to any vulnerabilities or potential **threats**, and draft a plan for how to address these concerns. This plan should include provisions for how staff will be coached on data security protocols and should be revisited regularly to mitigate potential new risks, particularly at key moments, such as when new features are added to your data systems or when organisational polices or programmes change.

Small security steps for big impact

To begin, there are small changes we can make to our daily habits to bring an additional layer of security to our work.

- Set your computer, smart phone, or other device to **lock automatically** after a short time interval and require a password to log in.
- If **personal devices** contain or access sensitive data related to your work, secure them in the same way you would a work computer or device.
- Never include personal details in the **subject line of an email**.
- Do not post the network or password **information for your Wi-Fi** out in the open.
- Set aside one day each year for **file clean up**, wherein all team members take a quick inventory of all their records and dispose of old paper and digital files that are no longer needed (shred paper documents and securely delete digital files per guidelines on page 68).

Using encryption to secure digital data

In the same way that we take steps in our day-to-day life to protect our physical integrity, whether it be wearing a motorcycle helmet or locking our office doors at the end of the day, it is important we take similar measures in the digital realm. This is the basis for data **encryption**, the process by which data are hidden from or made inaccessible to unauthorised users. Once data are encrypted, they can safely pass through open, public networks without being compromised, though again, we must always remember that **security measures like encryption help reduce risk, but cannot eliminate it entirely**. (Note: This is an area in which the legal norms in your area of operation must be consulted as data encryption is unauthorised in certain countries.)

encryption:

the process of converting readable text (plain text) into text that cannot be read without a key (cipher text); essentially encoding a message so it can be unscrambled and understood only by authorised individuals

Ideally, unauthorised users would never gain access to your information in the first place, but encryption helps ensure that if data systems are compromised, the information is unintelligible to outsiders. There are various forms of encryption available both for data in transit (data being shared between users/devices) and data at rest (data being stored somewhere). All electronic devices accessing sensitive data should be encrypted, but the channels by which data are shared should also be encrypted with appropriate software. Many devices have built-in methods for encryption, such as BitLocker for Windows-based computers and FireVault for Macs. See **Consider your medium for sharing** on page 77 for suggestions on encryption software for sharing information.

Masking people's identities with unique identifiers

When storing sensitive data about individuals, it is recommended to remove identifying information such as names and government-issued ID numbers and substitute that information with a unique identifier code.

Other than complete destruction, which is not always an easy process with digital data, it is challenging to guarantee complete protection of the identities of data subjects captured within a particular data set. As public data proliferate and data analysis techniques grow more sophisticated, we must all be aware that it is increasingly possible to re-identify data subjects based on data that does not directly name them.

When storing sensitive data about individuals, it is recommended to remove identifying information such as names and government-issued ID numbers and substitute that information with a unique identifier code. This could be a randomly generated number or string of characters, though it could also be an empowering opportunity to allow the client to choose a pseudonym that they like. In the case of the latter, it is a good idea to use this name anytime you are discussing the client in person or over electronic communication with your colleagues to help cement the norm. A key that matches the unique identifier code/name with the original names information should be encrypted and stored securely, separate from the full data set. Access to the key should be strictly limited to those who need it, ideally a very limited number of people in a given organisation. It is also important to remember that an individual can easily be identified by information other than their name.

The following details are a sampling of what could also be considered unique identifiers and, particularly in combination, can make it easy to ascertain an individual's identity.

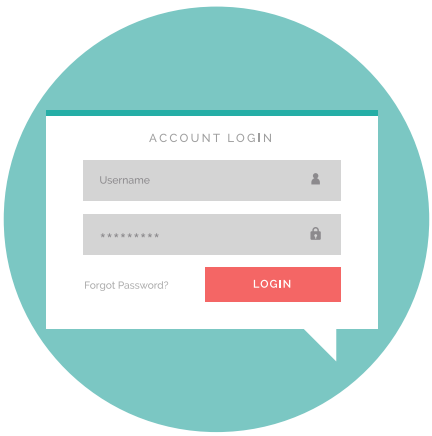
1. Names
2. Specific geographic localities
3. Dates directly related to an individual, including birth date or dates of service
4. Telephone numbers
5. Physical or email address
6. Government-issued ID number
7. Medical records and other account numbers
8. Biometric identifiers, including fingerprints and voice recordings
9. Full face photographic images

Passwords and passphrases

Passwords can be thought of as the digital version of your fingerprint in that it is something unique that belongs only to you. Within an organisation, even if sharing a device, it is useful for everyone to have unique log-in credentials and passwords to track data access (many digital data systems catalogue who is logging in when and from where, and which files they are accessing). When selecting a password or **passphrase**, we are attempting to both thwart others from guessing our password and prevent hackers from using technology to crack it, which can be done in a matter of minutes for simple passwords. As such, passwords and phrases must be increasingly long, unpredictable, and complex, meaning there is a mix of character type (numbers, letters, special characters like "!?@") and CaPiTaLiZaTiOn.

passphrase:

a string of words that is easy to remember, but do not naturally fit together



Here are some general password tips:

- At least 14 characters
- Include UPPERCASE letters, lowercase letters, numbers, and special characters (avoid putting symbols only at the beginning or end of your password)
- Set calendar reminders to change your password on a regular basis (such as every three months)
- Never share your passwords, even with trusted colleagues (if for some reason you must share a password, change it to a temporary password first and then change again after, and consider sharing the credentials through separate channels, such as username over encrypted email and password over encrypted text message)
- Passwords should not be associated with any personal information, such as family names, birthdays, etc.
- Use different passwords for different accounts
- Change your password immediately if you feel it has been compromised

If you are overwhelmed by the number of passwords you must remember, password managers such as Dashlane can be useful tools, but should be used with caution as they are also a target for hackers. These applications automatically generate strong, unique passwords for your various applications or services and help you store them securely by using a strong master passphrase to control the full account. If physically recording passwords is the best option you have, ensure it is in a well-secured, not obvious location.

An added layer of log-in security

You may have heard of dual- or two-factor authentication systems, in which a user's identity must be verified through multiple methods, typically by entering a password/phrase (something you know) and also confirming access through a secondary device or **biometrics** (something you have). For those using Google services, they offer 2-step verification. For organisations that use social media, Facebook and Twitter also have policies for implementing login verification. Multi-factor identification is an effective security strategy (Duo offers such services), but again, we should only implement security systems that are practical for our teams.

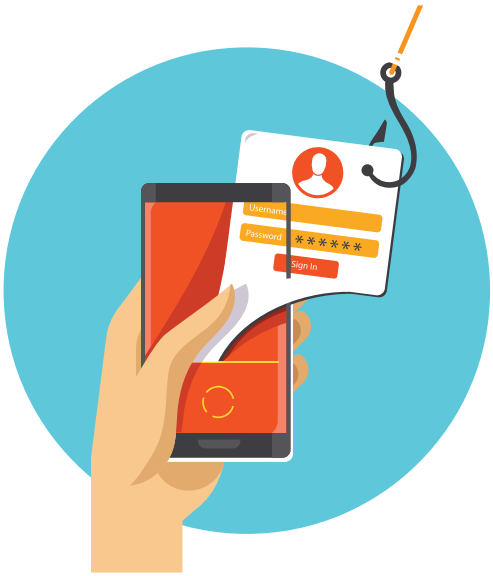
biometrics:

information on a person's physical attributes – such as fingerprints, retina scans, and voice recognition – that is often used to verify their unique identity

A note on biometrics: Biometrics is essentially the measurement and analysis of the physical qualities that make a person unique. For example, many smart phones today use fingerprints to verify the identity of the person using the device – this is biometrics. Given that anti-trafficking practitioners are sometimes working with communities without official government identification or tracking people across borders where language differences can make it difficult to confirm identity, there will no doubt be interest in using biometrics to alleviate some of these challenges. Before such measures are considered within the anti-trafficking space, there will need to be in-depth conversations with relevant experts around how we want to use such data and how we can guarantee they are adequately protected while not posing unintended harm.

Keeping bad actors out of your accounts

One of the most effective and common ways for hackers to gain unauthorised access to your organisation's digital infrastructure and data is through phishing emails. **Phishing** describes emails that look to be from a trusted source, but in fact come from someone attempting to trick you into sharing private information such as account passwords. Typically this is accomplished by including a link that appears valid, but redirects to a fraudulent website where any information you enter will be stolen and used to access your accounts.



Below are several clues you can look for to try to identify a phishing email. If you suspect an email may indeed be a phishing scheme, it is best not to open it, but instead communicate directly with the person or entity it claims to come from and ask if they recently contacted you.

- An email from someone you do not normally correspond with, even if you recognise the person's name
- If the email contains a hyperlink, check to see if the link connects to a **URL** different from the one being displayed (this can be accomplished by hovering over the link with your mouse, but it is important that you DO NOT CLICK the link)
- Requests for personal information, particularly account log-in information such as username and password
- Use of informal language, excessive punctuation, or spelling/grammar errors
- Language that conveys a sense of urgency, such as warning of sudden changes to your account (perhaps a bank or email account)

Data deletion and wiping

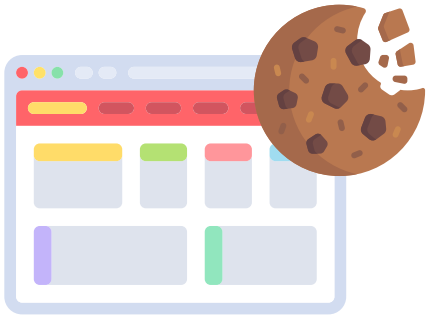
With confidential paper files, it is fairly obvious when data are destroyed (for example, through confetti shredding or incineration), assuming we know the location of all copies. **Deleting a file from your computer is not as straightforward.** Sending a file to the Trash or Recycling Bin is

URL:
the address of a website (often starts with www. and is preceded by http: or https:)

just the first step! Even after these receptacles are emptied, you are essentially only removing the file's name from the index of everything stored on your computer; the data remain until your computer saves other data in their place. The benefit of this process is you can often restore files you may have deleted by accident, but this also means users must be extra vigilant to securely remove data files they no longer want. To accomplish this, wiping tools are recommended to not only delete the information, but also mask its previous location and ensure any digital footprint has been removed. Such programmes like DBAN can also help with wiping temporary data, such as personal information input into website forms, account information, or **cookies**. Make sure you also wipe (erase) secondary devices, such as flash drives or digital cameras, after the requisite files have been accessed or downloaded. Of course, we can only truly erase data that is in our control; additional copies may exist elsewhere. NOTE: Bear in mind that personal data privacy laws in your area may affect your right to delete data.

cookies:

small bits of information about the websites you are visiting sent from your web server (what connects you to the internet) to your web browser (the portal you use to access the internet, such as Chrome, Firefox, Safari, Explorer)



Know the legal environment

National and regional legal frameworks should be consulted when designing data protection policies, particular for highly sensitive personal data. Entities must consider the laws not only of the localities in which they are registered, but also where they operate, where their data are stored (and pass through), and where their clients/subjects reside.

Finding comprehensive information on relevant legislation on digital data and cyber security can be quite challenging. Law firm DLA Piper offers some guidance on data protection laws at www.dlapiperdataprotection.com, though it is best to consult a lawyer with technical expertise on this subject for comprehensive understanding.

Entities must consider the laws not only of the localities in which they are registered, but also where they operate, where their data are stored (and pass through), and where their clients/subjects reside.

Have an emergency plan for data breaches

Develop a list of people to consult in case of a data breach or other security emergency that goes beyond your organisational expertise, whether that's legal or technical support. Similarly, make a plan for potential loss of a device that contains sensitive information. Should there be a security breach or other violation, it is critical that you notify data subjects whose data have been compromised and consider what protective resources you might provide them.

Secure your physical environment

Though data are increasingly digital, we are still working in physical spaces and must consider the security of our offices and work environments when making decisions about data collection. For example, working in a public setting is inherently less secure, as is connecting to public Wi-Fi networks. Consider small, but significant changes such as disabling preview mode for text messages and emails on your devices and setting short intervals for your devices to automatically lock when inactive.

Resources:

Security in a Box
(available in English, Thai, Khmer, Bahasa Indonesia, Burmese, and Vietnamese)
https://securityinabox.org/

Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes
The Cash Learning Partnership (2013)
http://www.cashlearning.org/downloads/calp-beneficiary-privacy-web.pdf

Girl Safeguarding Policy: Digital Privacy, Security, Safety Principles & Guidelines
Girl Effect (2016)
https://www.ictworks.org/wp-content/uploads/2016/05/GE-Girl-Digital-Privacy-Security-Safety-v-May-2016.pdf

WFP Guide to Personal Data Protection and Privacy
World Food Programme (2016)
https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

Anonymisation: managing data protection risk code of practice
UK Information Commissioner's Office (2012)
https://ico.org.uk/media/for-organisations/documents/1042731/anonymisation_code_summary.pdf

Digital Security Exchange
https://www.digitalsecurityexchange.org/

Responsible Data
https://responsibledata.io/

Electronic Frontier Foundation (various tools)
https://www.eff.org/pages/tools

Data Sharing

There is generally strong awareness within the anti-trafficking community of the risks of sharing data, particularly when it comes to personal information about potential trafficking victims or survivors (note: the same regard should be afforded to the personal information of any individual, including suspected traffickers). But less attention has been given to the **vast benefits of sharing information**, which include:

- getting to a more robust picture of the scale and scope of the problem of human trafficking

  At the micro level, an agency providing vocational training to a client might like to coordinate with those offering medical support to better tailor services to client needs. At the macro level, NGOs in sending and receiving localities might coordinate to better understand the trafficking process.

- making progress in efforts to de-duplicate data being reported by multiple entities
- limiting re/traumatization of survivors and avoiding the general discomfort of sharing sensitive, personal information with service providers when possible
- creating opportunities for specialization and resource sharing while minimizing duplication of efforts
- learning from the constructive scrutiny that comes from allowing others to review our work

Many argue that the competition over limited funding keeps us from sharing data, whether from fear of disclosing proprietary information and approaches or revealing gaps and weaknesses in our programmes. **But generally, if you are collaborating with the right people, you will find this kind of openness to be productive and beneficial to your work, not to mention it can contribute to a better understanding of the problem among the international anti-trafficking community.**

There are various methods for sharing data depending how widely you want it distributed. Task forces and consortia are useful mechanisms for determining what type of data other practitioners collect, their methods for doing so, and their policies on data sharing, allowing us to get new ideas and share best practices. If we wield the information we can glean from sharing good data, the anti-trafficking movement is likely to be able to draw more funding, both from private donors and central governments, to this issue. To ensure this goal is realised, anti-trafficking entities need not necessarily operate on the same data systems, but they must ensure their various methods are compatible and can communicate with one another (see Databases section on page 49).

While giving attention to protecting people's **personal identifying information**, there is tremendous value to be gained in enhanced collaboration within the anti-trafficking field. Many actors have realised this and are sharing information both through informal and official channels. For example, anti-trafficking police units might share case data across borders through mutual legal assistance treaties or NGOs providing legal assistance might coordinate with the legal system to ensure holistic services.

personal identifying information (PII):

any data that could be used to identify a specific individual; in addition to someone's name, PII can include their passport number, birth date, or address

Remember when sharing data that you must have permission from the data subject to disclose their information outside the organisation. Moreover, make sure the original intent of the data is respected and if sharing it opens it up to other uses or interpretations, additional consent must be received.

Oftentimes this exchange is happening casually in face-to-face conversation, over email, or through instant messaging platforms such as WhatsApp (see Data Security section on page 61). Though it is important to encourage such cooperation, it is important that protocols are established to govern why, how, when, and with whom such data are shared. Fortunately, technological advances have enabled new platforms that make data sharing easy, fast, and secure.

Create a data-sharing plan

A critical first step in approaching data sharing is creating a data-sharing plan for your organisation that addresses the core questions below. It is helpful to appoint a key person within your organisation who oversees and is accountable for these processes. Similarly, if you are part of a larger consortium of organisations, ensure there is a lead person or entity in charge of preserving and protecting your shared data. Having a documented plan will ensure everyone within your organisation follows the same norms and standards. Like anything else, think of such standards and processes as a starting place from which to adapt over time as the environment changes.

- What data will be shared and in what form?
  If raw data will be shared, as opposed to simply summary statistics, we must ensure it is properly redacted or altered to ensure private information is protected.

- What data documentation will be shared along with the data to help inform its accurate interpretation?
  This includes metadata and other key information on how data were collected or may have been altered over time.

- With whom will your organisation share data?
  Data should be shared as widely as makes sense, but always in a way that protects the privacy of data subjects and is consistent with relevant laws and regulations in both the jurisdictions of the sender and recipient. You can consider having different protocols for different recipients, informed by the level of trust and perceived privacy.

- How will you determine what data are appropriate to share?
  Just as you should not collect data that you do not use in your programming or analysis, you should not share data without a clear understanding of why someone else needs it and how they will use it. Moreover, as discussed below, data de-identification is not a simple process so it is important to ensure data is truly anonymised before sharing widely.

- How will the data be received and accessed?
  Consider what format makes data most easy to process and analyse. If digital, a .csv file may be the most appropriate file type if data is meant to by analysed or manipulated, whereas a locked .pdf may be best for data that is only meant to be viewed.

- How will sender and receiver ensure data are protected in transit and long term?

Note: Consider implementing an agreement among your team, including volunteers and short-term contractors, that acknowledges both the value of and potential concerns associated with data sharing and outlines best practices to keep data protected and confidential. Lastly, they should attest that any organisational data stored on their personal devices must be deleted upon termination of their affiliation.

Draft a data sharing agreement

For information being shared privately between entities, it is recommended you implement a data sharing agreement or non-disclosure agreement (NDA) between your organisation and any outside entities with whom data will be shared that outlines proper data use and security protocols, , and is mindful of applicable laws in relevant jurisdictions. Core elements of such a document should include, but are not limited to:

- A clear description of how the recipient will use the data
- An indication that ownership remains with the organisation sharing the data (and of course the data subjects)
- Recipient must agree to use the data for the purposes outlined therein and not to disclose, release, sell, or otherwise grant access to that data to other parties
- A clear description of how the recipient will ensure the data remain confidential, including how they will maintain control of the data; if data are accidentally disclosed by the recipient, this should be reported immediately to the sharing entity
- In the case of de-identified data, the recipient shall not make an effort to re-identify the data subjects
- Stipulated timelines for data use and destruction

Protecting the identity of data subjects

Data de-identification is the process by which you prevent a person's identity from being connected to their data – and it is by no means straightforward. For example, removing or obscuring someone's name from their record (see Unique Identifiers on page 64), but retaining other demographic information such as birthdate/age, city of residence, or personal identification numbers can make it easy to identify that individual. Given the high potential for stigmatization, retaliation, or other harm to trafficking survivors in particular, this point

is critical. As covered above, anytime data are shared, we must consider the perspective of the data subjects and how it might affect them if the wrong person accessed those data.

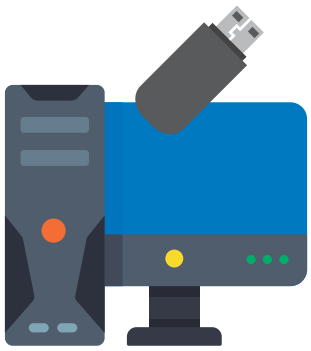
Here are some guiding questions to help you decide if data are in fact PII and therefore may need to be aggregated (grouped into summary statistics not connected to individuals) or de-identified before sharing, depending on level of trust and security.

As covered above, anytime data are shared, we must consider the perspective of the data subjects and how it might affect them if the wrong person accessed those data.

- Can an individual be identified from the data directly, or, from the data when combined with other relatively accessible information?
- Do the data obviously relate to a particular individual?
- Could the data be used to directly impact or affect actions or decisions related to an individual?
- Do the data focus on the individual as the central theme, as opposed to an event or other subject matter?

If the answer is "yes" to any of these questions, you are likely dealing with PII and need to de-identity or aggregate your data before sharing widely. Also keep in mind that data related to a smaller population, say the residents of a specific village, may need to be specially protected because it is possible the identities of subjects could be easily guessed by looking at other data variables knowing there are so few people in that place.

Consider your medium for sharing



Different methods for sharing information offer unique benefits and potential drawbacks. **The core element of data sharing is trust** – knowing the person with whom you are sharing that information well and trusting that they will treat the data securely, including by not sharing it further without permission.

Perhaps the most basic option is to **physically share** paper files or transfer digital files on an external hard drive, USB key, or other external storage device. This method provides a lot of security in that you know precisely who is receiving the data, but it opens opportunities for the records or devices to be lost or stolen, and could potentially threaten the physical security of the messenger.

Text messaging, ideally through an app with **end-to-end encryption** (see **Data Security** on page 61), is a good option in terms of ease, though users should be verified and practitioners should avoid sending sensitive data, particularly in chat groups that may include people they do not know well. WhatsApp and Signal both employ the same encryption methods, though Signal does not store metadata on its chats and is **open source**.

Sending information over **regular email** is not a very secure method as many email providers can be easily hacked. Again, encrypting files before sending can help avoid this problem; it is recommended that encryption keys be shared over a secondary, secured medium. For example, there are several plug ins available that enable encryption for Gmail users, such as Virtru and FlowCrypt, and encryption can be enabled for users of Outlook 365. Using an encrypted email service such as Mozilla Thunderbird is also an option, though it requires an investment of time to set up properly on both ends.

Using **cloud services** like Dropbox, CertainSafe, iCloud, Microsoft OneDrive, and Google Drive are a convenient mode for sharing information and can be made more secure by encrypting the data files before uploading them to the server. Data management with such platforms is important; permissions need to be actively managed to ensure only appropriate team members can access specific files necessary for their work for an appropriate period of time (the project period, for example).

end-to-end encryption:

communication that ensures only those you are directly communicating with can read the messages; information is hidden even from the provider of the service

open source:

software for which the source code is freely available to the general public for possible modification or redistribution

Data Analysis and Interpretation

Bits of unprocessed data stored in files, spreadsheets, and databases, are disparate and difficult to understand from a macro level. They need to not only be analysed to answer key questions about our work, but also presented in a way that people can quickly and easily comprehend (more on that in the **Data Presentation and Visualisation** on page 89).

We can use data both to internally evaluate the efficacy of our work as well as to tell stories to the general public about why that work is important. We can use them to shape policy and measure the effectiveness of programmes to serve survivors.

Data analysis and interpretation do not necessarily require cutting-edge technology or complicated software, or even advanced training. **The most fundamental requirement for good data analysis is a sense of curiosity – a commitment to understanding the who, what, where, when, why, and how of human trafficking**. The ideas and tools herein can help us to begin answering these questions. Moreover, investing in these highly valuable skills is very likely to pay off throughout your career.

As we've emphasised throughout, data are a necessary building block in all arenas of the anti-trafficking movement. We can use data both to internally evaluate the efficacy of our work as well as to tell stories to the general public about why that work is imperative. We can use them to shape policy and measure the effectiveness of programmes to serve survivors.

For the most part, information shared publicly by the numerous anti-trafficking entities working in Southeast Asia – globally, in fact – often centres on the number of (reported, investigated, or prosecuted) cases or the number of people served (community members for prevention and survivors for protection) by a given programme, sometimes broken down by basic demographics such as age and gender. The other type of data we often see is related to M&E, typically linked to the reporting

requirements set by donors, or requested by governments, task forces, and international bodies (such as the United Nations Office on Drugs and Crime or the U.S. Department of State's Office to Monitor and Combat Trafficking in Persons).

These aggregated numbers are certainly useful and important, but they are only part of the picture. Not analysing the vast amounts of information that many of us have access to (or not collecting it in the first place) is a missed opportunity. We can do more than tabulate cases once a year or fill in a log frame periodically to outline how we hope to create impact through our programmes. **Real impact requires a commitment to learn from, and not simply report, these data.**

For example, data on the number of survivors a given organisation has served could be further analysed to track how many cases social workers on average can handle at a given time to inform how work is distributed among a team. Or when reporting on investigations, law enforcement could track what industries victims are typically trafficked into to better understand what makes a given type of business susceptible to exploitation, enabling us to also focus on prevention. Of course, to do any such data analysis well, we need to have reliable, accurate data to examine in the first place; otherwise we may draw inaccurate conclusions and design interventions and policies around bad information.

This section aims to share some foundational ideas on how to approach new and expanded forms of data analysis among your team. **In addition to supporting career advancement, investing in these skills will ensure that we better understand the intricacies of human trafficking, and that we can communicate them more precisely and effectively to stakeholders.**

Follow the scientific method

As emphasised throughout, the intended purpose of any data system should be set prior to such systems being built. The same is true of **research design**. One should have an idea of the questions they'd like answered before embarking on data collection. This essentially means setting a research question at the outset, perhaps making a prediction of what you think you may find, and selecting an appropriate method for collecting the information you need to evaluate this question. From there, you can start gathering your data and analysing it to draw conclusions in line with your original research question.

research design:

the overall approach to the various components of study, from data collection to analysis, laid out in a thoughtful, coherent, and logical way

A primer on statistics

This branch of mathematics can be very practical and accessible – it focuses on the interpretation of data. Most of the statistics we see in the anti-trafficking field are **descriptive** in nature, meaning they describe or summarise data in a way that allows understanding of trends and patterns. Again, this information is certainly useful to understand *what* is happening with regard to human trafficking, but it cannot tell us anything about *why*.

For example, the 2016 UNODC Global Report on Trafficking in Persons noted that 52% of detected victims of trafficking in Thailand in 2014 were girls[1]. This tells us that about half of detected victims are girls, but it does not necessary give us insight into why girls in Thailand are vulnerable to human trafficking.

For quantitative data, the most commonly reported characteristic of any given dataset is its midpoint (**central tendency**, in technical terms). This is thought to be the point around which most observations cluster and you will find it commonly reported as the **average**, **mean**, or **median** of a given sample.

For example, anti-trafficking organisation Polaris reported in 2016 that the average age of entry into the commercial sex industry among the 123 survivors they interviewed was 19 years[2]. Others have claimed to be able to quantify the median price of a slave[3], but the methodology behind this calculation is unclear, calling into question its validity.

Note: The mean is more sensitive to extreme values when compared to the median as it takes into account the magnitude of each observation.

[1] https://www.unodc.org/unodc/en/frontpage/2016/December/almost-a-third-of-trafficking-victims-are-children_-unodc-report.html
[2] https://polarisproject.org/blog/2016/01/05/average-age-entry-myth
[3] https://bits.blogs.nytimes.com/2013/03/06/global-slavery-by-the-numbers/

descriptive statistics:

data analysis that describes, demonstrates, or summarises data in a way that allows understanding of trends and patterns

central tendency:

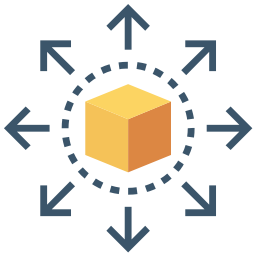
the typical or central value for a given quantitative indicator

average or mean:

the sum of all the observations divided by the number of observations

median:

the middle point if all the observations are ordered numerically from smallest to largest (or the average of the two middle points for a dataset with an even number of observations)



We might also be familiar with measures of **spread**, which give us information on the breadth of the observations of a given variable. For example, we could observe that in a given jurisdiction, trafficking survivors receive anywhere from $100 to $1,000 USD in restitution. $100 to $1000 would represent the **range** of this variable.

*Note: We might see the terms **variance** or standard deviation used in more complex statistical analysis; these are also measures of spread.*

Another area where we have likely dealt with statistics is programme evaluation, such as understanding our success **rate** (as measured perhaps by the extent to which we have reached our intended goals). We could also compare performance over time or across different geographies.

Much of the data analysis within the anti-trafficking field is based on non-experimental research, meaning we are studying a naturally occurring phenomenon involving two or more **variables**. This means the researcher is not controlling or manipulating what is happening. In other words, we are simply observing and drawing conclusions from what is happening around us. For example, a justice ministry might like to know how long it takes a human trafficking case to be adjudicated in a given jurisdiction or a journalist might investigate which seafood producers are using forced labour in their supply chains. Likewise, civil society organisations might analyse their data to know what percentage of identified trafficking survivors is being supported with vocational training.

Other forms of analysis that can be employed are tests of group differences, essentially comparing multiple samples (such as different age groups, people in forced labour across

spread:

the full array of values for a given quantitative indicator

range:

the difference between the largest and smallest value for a given quantitative indicator

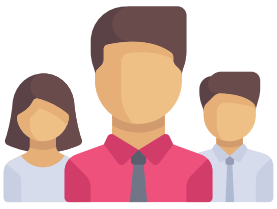
variance:

a measure of how far a set of observations deviate from the average

rate:

the frequency of a given phenomenon

variable:



a specific characteristic of the data subject, such as gender, age, nationality

different sectors, or people using different forms of transit), and tests of association, which is looking for an association among multiple variables within a single sample (for example, is there an association between someone's migration route and a specific form of exploitation).

When analysing any data, it is important to keep in mind that we cannot draw conclusions about an entire population beyond the sample we have observed and analysed. Since the full **population** of traffickers and victims is unknown, we are merely describing what we've observed among a select group of people that is not necessarily reflective of the entire population.

For example, a sample would be the companies identified in an *Associated Press* story about forced labour in the fishing sector; the population is all known and unknown companies employing forced labour in the fishing sector.

Another example, in 2015, IOM reported that 88% of the trafficking victims assisted in the ASEAN region were male and that 7% were trafficked for purposes of sexual exploitation[4]. Notice something very important here – IOM did not claim that 88% of *all* victims of human trafficking in Southeast Asia were male, just those their organisation assisted.

IOM is not claiming that this sample is necessarily representative of the full picture of human trafficking in the region; there may be reasons that this organisation in particular received more male victims of labour trafficking, whereas other entities focused primarily on sex trafficking or serving female victims would likely see a very different picture. This is where the concept of bias comes in.

[4] https://www.iom.int/sites/default/files/infographic/ASEAN-CT-Infographic-05july2016.png

sample:

the subset of the population that is being observed/whose data are being collected

population:

the entire group under investigation

When analysing any data, it is important to keep in mind that we cannot draw conclusions about an entire population beyond the sample we have observed and analysed.

Bias is not by default a bad (or good) thing; it is simply a reality that most of us have pre-existing perceptions or biases related to what information and populations we access in our day-to-day work.

Data become impactful and persuasive when we can use them to identify **trends** and **patterns** (and **outliers**) – and to then tell stories about what that information reveals. Here are some general phenomena to look out for when doing data analysis:

trend:
For example, a civil war or natural disaster could lead to changes in migration trends, which might be used to decide where we want to strengthen trafficking prevention strategies.

patterns:
For example, we might note based on a pattern among observed samples that girls across the world, no matter their location or demographics, are less likely to be trafficked if they have completed secondary education.

outliers:
For example, if we are trying to understand forced labour in the textile industry in a given state, we might observe a factory with no reported cases of exploitation. It would be useful to understand what makes it different – it could be an indicator of better labour practices or that employees are so scared that they do not report cases or just that nobody ever collected the information in the first place. Either way, we will likely benefit from analysing this case further.

gaps:
For example, if we have data on all but a few localities in a given state, what can we learn from understanding why those data do not exist. Perhaps they could not be collected owing to a natural disaster in that area or perhaps there are no community members with resources to collect that information.

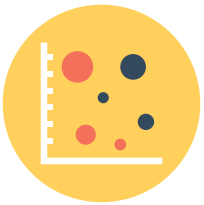
trend:

a pattern of change or general tendency observed across data points

patterns:

groupings and sequences that arise when comparing people, objects, and events

outliers:



data points that clearly do not fit into existing trends or patterns

gaps:

where are there holes in our data and what do those missing pieces reveal

positive deviance:
For example, having a community leader who is engaged and well-informed on the issue of human trafficking might make their community more effective when it comes to prevention strategies.

Confront your bias

We all have inherent biases that affect the way we understand information. Being aware of how such distortions can affect the data we access in the first place and how we understand the resultant information is a critical first step in ensuring we minimise the effects bias can have on our final product. For example, for a long time, the anti-trafficking community had a bias toward combatting sex trafficking, which was largely seen as a phenomenon that disproportionately affects women and girls (with less focus on labour trafficking). Such a bias can inadvertently encourage law enforcement, for example, to identify more female victims because that is the victim profile they are focused on, which then further feeds into the original bias.

positive deviance:

an approach to behavioural and social change based on the observation that in any community there are people whose uncommon, but successful behaviours or strategies enable them to find better solutions to a problem than their peers, despite facing similar challenges and having no additional resources

For example, having a community leader who is engaged and well-informed on the issue of human trafficking might make their community more effective when it comes to prevention strategies

Sample size matters

Often in data analysis, we are looking for big changes based on the idea that the public finds them more compelling. Unfortunately, this leads to the tendency to claim significant differences over time or between groups, when in fact the total numbers are too small for meaningful comparison. The general rule is that you want a sample size of at least 50 observations (whether that's incidents, people, cases, etc.) to draw meaningful conclusions about change.

The best practice is to be honest about your data and how you present it to the public. For example, if the counter-trafficking task force in a given country meets two times one year and four times the next, one could claim a 100% increase in number of meetings, but this is not nearly as significant as having weekly meetings one year and over 100 meetings the following year. Similarly, if a NGO assists 10 trafficking survivors with unconditional cash transfers one year and 12 the following year, they can claim a 20% increase when the difference is only two people.

Moreover, context is very important for properly understanding statistics. For example, between 2008 and 2012, there was a 40% increase in the number of countries criminalizing most or all forms of human trafficking as defined in the Palermo Protocol, whereas the increase was 16% between 2012 and 2016, according to UNODC[5]. Though the latter number may sound less impressive, we would expect a large upswing in criminalization in the years following adoption of the Palermo Protocol, and thus it is still quite significant given 88% of countries have now criminalised all or most of these offences.

The golden rule of statistics

Lastly, in the case that your work goes beyond descriptive statistics to include **inferential statistics**, such as the work behind the Global Estimates of Modern Slavery, for example, it is important when analysing our data that we do not assume that correlation among variables, meaning they occur in tandem or appear to be related in some way, indicates a causal relationship.

*A common example is that smoking cigarettes is **correlated** with alcoholism, meaning people who smoke a lot also often drink a lot, but we would not say smoking causes alcoholism. That said, medical research supports the statement that smoking directly causes users to be at higher risk for developing lung cancer.*

Correlation can be caused by a number of external factors or may simply be a coincidence. When presenting your findings, it is important to be explicit about the facts and not imply causality where it is not confirmed to exist. Similarly, we should keep this in mind when interpreting other people's data.

inferential statistics:

data analysis that makes informed guesses about an entire population using data drawn from a sample of that population

5 https://www.unodc.org/documents/data-and-analysis/glotip/2016_Global_Report_on_Trafficking_in_Persons.pdf

Resources:

DataBasic
https://databasic.io/

NOTE: DataBasic offers tools to quickly analyse your data, but do keep in mind you should not upload any sensitive information to such websites. For any outside service, be sure to review the Terms of Service prior to sharing any information.

School of Data
https://schoolofdata.org/

Data Presentation and Visualization

Now that we've gone through all the work of carefully collecting and analysing our data, we are ready to share the information we have produced with the rest of the world in a manner that is equally thoughtful and thorough.

As data keepers, we bear a responsibility to critically interpret and accurately reflect the true nature of the data we use in any reports, brochures, websites, graphs, or other media we create. When working to combat a problem as complex – and often misunderstood outside the field – as human trafficking, we will likely have to rely on a mix of quantitative data and qualitative data to communicate our message effectively. We all want to draw more public attention to this issue, but we must also be careful to present factual information that is not exploitative to **guarantee the movement's credibility**.

As data keepers, we bear a responsibility to critically interpret and accurately reflect the true nature of the data we use in any reports, brochures, websites, graphs, or other media we create.

Both quantitative and qualitative information based on good data are persuasive in their own way, as are individual narratives. **Together, the picture they paint can be used to engage relevant parties, from the news media, to titans of industry, to academics, to the philanthropic community, to local communities.** An added benefit of collaborating across the anti-trafficking movement is you have a built-in network of peers to advise and guide your work, as well as a receptive audience for any research you share.

Visuals, including images, infographics, and charts, can be very influential and help make data more accessible to consumers. If done well, good data visualisation communicates information quickly and makes it easier to understand. Because many practitioners in Southeast Asia are already using Excel to manage and manipulate their data, this can be a good starting place for creating graphs and charts. There are many other software options available that are focused on making it easier to visualise and understand data, such as Tableau. That said, do not feel like you have to use a visual if it does not suit the data. Sometimes a written narrative is the most accurate and compelling form of communication.

If you are distributing content online, remember that your report and any graphics may be viewed across multiple devices (printed on paper, computer, phone) so it is best to format them to be compatible across media.

Engage survivor leaders in outreach

Human trafficking survivors have very important and valuable expertise to share and have generally been under-appreciated as critical members of the movement. Any time we are considering asking survivors to share their stories and perspective publicly, whether in person or in printed or digital materials, **there are many things we need to keep in mind to ensure we are applying a trauma-informed approach while acting in their best interest and providing a platform of empowerment, as opposed to further exploitation.** Here are some key ideas to keep in mind as you approach this:

- Survivors must retain full control over how and when their personal information is shared and should not be compelled by a case manager or other service provider to participate in outreach. Generally minors should not be asked to participate.

Integrating a dashboard that automatically generates graphs from your real-time data within your database may be a helpful way to encourage your team to appreciate the value and utility of data visualisation.

- Consider ways other than a survivor sharing their personal trauma history for them to participate in outreach efforts, such as helping to plan a media campaign or offer key insight during the data analysis process. They should be appropriately compensated for their time, including speaking engagements. If relevant to your organisation, this may be an area for professional development/vocational training.
- Cultivate opportunities for survivors to share stories of resilience and strength.
- Avoid presenting stereotypes or overly dramatised depictions in your outreach, such as minimally clothed women and children or people with their hands or mouths bound. Be aware of how what you present could stigmatise certain communities or cultures.

Use of imagery

Anti-trafficking practitioners, advocates, and researchers should give special consideration to how they present imagery on websites, in printed publicity materials, and in reports. These materials are important opportunities to challenge existing stereotypes of who is a trafficking victim as well as present more empowering imagery.

When considering taking and using someone's photograph, first consider how you would feel if you were photographed in a given situation as well as cultural norms around capturing someone's image. **If you move forward, you must obtain consent**. It is advised to take photographs that hide people's faces or other identifying features. You might also consider focusing on situations of empowerment (not just exploitation), such as survivor leaders sharing their expertise. Depending on the context, it might be best to use animations or drawings with limited identifying features as opposed to photographs.

Again, images should only be used in a way that reflects the original purpose to which the subject consented; additional consent should be given for other uses.

Again, images should only be used in a way that reflects the original purpose to which the subject consented; additional consent should be given for other uses.

Include signposts for data interpretation

As emphasised throughout, perfect information is impossible. The best we can do is to try to make sense of what data we do have, which requires a close examination of their quality. When packaging this information to share with others, it is helpful to include relevant context to ensure their understanding is as factually accurate as possible. For research reports, this comes out in the methodology section (where we describe our approach and actions taken to answer a research question), but we also need to establish context in more informal publications as policymakers, donors, and other influencers frequently consume these.

For example, be sure to include the time period covered or the geographical reach of any statistics or other information presented. **Limitations and biases in how data were collected and interpreted should also be acknowledged.** If data could not be collected in certain instances, say so and explain why, if possible. For example, perhaps it was an emergency situation or we had to rely on a convenience sampling, meaning collecting information from those that are easiest to reach.

The difference between observed cases and all cases

A pervasive challenge across any organisation, whether combatting human trafficking or not, is the tendency to conceive and describe their understanding of their work as the complete picture, but this is rarely if ever the case. For example, if a NGO claims that 75% of trafficking cases have female victims, what they might really mean is that 75% of the cases they've worked on or come into contact with had a female victim. But as we learned, we all have biases in our approaches to our work and how we understand the results, whether based on our funding structures, the background and expertise of our staff, our geographical setting, our personal demographics, or other quality. As such, it is important to make this clear in publications by using words like "observed cases" or "our clients." For example, as opposed to "victims of forced labour spend an average of two years in their trafficking situation," we might say, "of the cases our organisation observed, the average length of time in a situation of forced labour was two years." This is relevant to the difference between a sample and a population, as previously discussed on page 83.

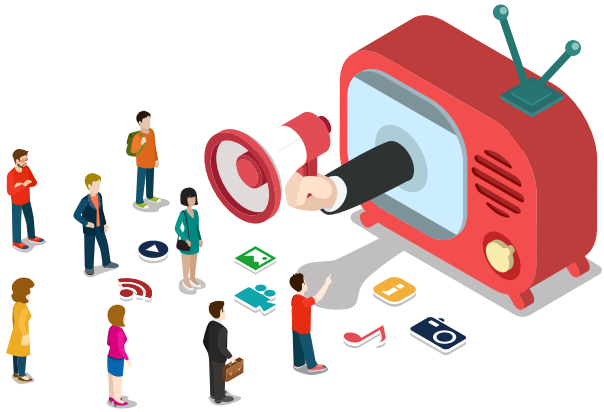
Devise an outreach strategy

Many organisations do not have the benefit of a dedicated media and communications team to help spread the message about their work and share achievements and publications. That said, communications (some might call this public relations or marketing) are an important tool in supporting the success of the anti-trafficking movement. **In order to get others to appreciate the gravity of this problem and take appropriate action, we must effectively persuade them to care. We can most readily do that by sharing honest information about the problem, our programmes, and how we might work to curb human trafficking.**

Here are some simple steps we can all take to develop an effective communications strategy:

1. Map your stakeholders.

It is important to know the audience well so that messages can be tailored to meet their needs and framed in a way that resonates. Brainstorm all the possible consumers of your print or online materials and ensure you shape your outreach to meet these distinct profiles. Think through any connections you might have to local and international influencers who would be interested in promoting your work through the media or elsewhere.



2. Determine your main messages.

As we know, people are easily distracted and can be overwhelmed by too much information. It is best to select a few key learnings that arise from your data and craft outreach around them. It is helpful to ground this in the context of how your organisation is uniquely placed to address or promote these lessons; in other words, how does this information connect with your overall mission and strategy? Lastly, it is important to ensure these messages are used consistently across your various media platforms, from websites to social media to printed materials to interviews. Distributing a press release is a good strategy if you have a discrete achievement or finding to share with the news media; be sure to include relevant background information about your organisation and key contacts available to be interviewed. There may even be opportunities for you or someone at your organisation to contribute an editorial to a local newspaper or write a contributed story for an online outlet in an effort to promote your work.

3. Keep it fresh.
As people are exposed to increasingly more information through the proliferation of social media, we must find new ways to make our messages stand out. This means not only presenting thoughtful, accurate analysis, but also striving for regular updates to ensure audiences stay engaged. It may be helpful to establish a timeline each calendar year for releasing reports and other print or digital materials.

4. Social media presence.
Blogs and social media, including Facebook and Twitter, offer opportunities for reaching wide audiences creatively and cost-effectively. These platforms can be well suited to sharing key messages, reports, and research findings that you want to be widely circulated, but they are not appropriate for more sensitive communication.

The medium is the message

Data visualisation can be a powerful way to communicate your data in a way that makes it easy to understand and memorable. There are numerous methods for visualising data, each with its unique benefits and potential challenges. These could include basic tables, bar charts, pie graphs, scatter plots, cartograms, word clouds, heat maps, and more! Just remember, **clarity is more important than being flashy;** in other words, resist selecting a certain type of chart or graphic just because it is attention grabbing or colourful. Though a complex graph or colourful image might draw someone's attention, it might make it difficult to understand the information it aims to convey.

Generally, data visualisation aims to communicate, for example, general trends and distributions, relationships between variables, changes over time, and differences among different sample groups. For example, if you are trying to compare values in a given data set, such as the number of trafficking cases reported by geographic region, a bar chart might be a good choice. If you are trying to understand how individual components make up a whole, such as what percentage of trafficking victims are adults v. children, a pie chart or stacked column graph might be best (note: order segments according to their size and ensure that the sum value adds up to 100%). For distribution, meaning understanding trends

Data visualisation can be a powerful way to communicate your data in a way that makes it easy to understand and memorable.

and the range of values, as well as noting outliers, a scatter plot might be best.

No matter the type of chart or graph:

- Include title that a clearly and succinctly describes what is being presented, including what time period and geographical space the data represent
- Clearly state the unit of measure of all included variables (duration in days or years, for example) and ensure the scales fairly represent them (ideally beginning each axis at zero)
- Always give the data source
- Choose colours deliberately

  Remember that colours can have implicit associations, such as the red ribbon for AIDS/HIV awareness or orange being associated with campaigns to end domestic violence. At times, varying shades of the same colour might make the most sense (darker shades typically indicate a higher concentration of a given characteristic), though grayscale might make sense as variation of these shades can be easier for the human eye to detect and differences will be clear even if a document is printed in black and white.

Resources:

Guidance Note on Use of Victims Images
Freedom Collaborative (2016)
http://ethicalstorytelling.com/wp-content/uploads/2017/09/Guidance-Note-on-Use-of-Victims-Images_final.pdf

Social Media Handbook: Tips for Civil Society Users
Cooperation Committee for Cambodia, in partnership with USAID's Development Innovations (2017)
http://www.development-innovations.org/wp-content/uploads/2017/10/Social-Media-Handbook-EN-High.pdf

Visualizing Advocacy (various visualisation tools)
https://visualisingadvocacy.org/resources/visualisationtools

Canva
www.canva.com

Piktochart
https://piktochart.com

Infogram
https://infogram.com

Concluding Thoughts

Throughout this research, the team was continually humbled by the dedication of the dozens of frontline anti-trafficking practitioners interviewed across Southeast Asia. These Getting to Good Human Trafficking Data guidelines aim to be a resource to support that effort to combat human trafficking, motivated by the passionate belief that good data are essential to achieving our shared goal. As emphasized throughout, there are many yet unanswered questions about the nature, scale, and scope of the problem, and until we have higher-quality, localised data, implementing effective policies and programmes – and being able to evaluate their impact – will remain a significant challenge.

There is no single, perfect database that can answer all of our questions, but by working as best we can to strengthen and standardise our approach to data collection, we will encourage comparability of data across the movement. We are hopeful that we've demonstrated the critical role data can play in our work, while offering practical tools and guidelines to support the implementation of practices that get the movement closer to its intended impact.

Ultimately this document serves as a catalyst to assess and enhance existing data collection efforts – tailored to the local context with a view to the regional potential – for good, responsible data to combat human trafficking. Again, we realize that not every section of these guidelines can be relevant to the diverse types of work we are all undertaking, but we hope the seven data principles resonate and that you are able to integrate some of the recommended practices and approaches into your organisation's day-to-day operation. After all, you are the leaders in this fight.

About the Human Rights Resource Centre

The Human Rights Resource Centre is a non-profit academic centre headquartered at the University of Indonesia in Jakarta, with a partnership network throughout Southeast Asia. The Centre is currently active in seven out of 10 member states of the Association of South East Asian Nations (ASEAN). The Centre was established in 2010 by several of the original members of the Working Group for an ASEAN Human Rights Mechanism, as well as other prominent regional human rights advocates and academics, all of whom have been engaged in the protection and promotion of human rights for several decades. The Centre has been accorded consultative status by the ASEAN Intergovernmental Commission on Human Rights (AICHR) in November 2016.

The Centre was established to foster an institutional network that would produce high-quality, independent, research on human rights issues of most pressing concern to ASEAN and aims to shape the discourse on human rights in ASEAN. The Centre also supports the human rights agenda of the AICHR, especially through public education, research and training programmes. Through pedagogical initiatives with partners both within and outside ASEAN, the Centre hopes to build the capacities of researchers, promote knowledge exchange, and support the protection and promotion of human rights in the Centre's core thematic areas. These are rule of law, business and human rights, and the rights of vulnerable populations.

About the East-West Center

The East-West Center promotes better relations and understanding among the people and nations of the United States, Asia, and the Pacific through cooperative study, research, and dialogue. Established by the U.S. Congress in 1960, the Center serves as a resource for information and analysis on critical issues of common concern, bringing people together to exchange views, build expertise, and develop policy options. The Center is an independent, public, nonprofit organisation with funding from the U.S. government, and additional support provided by private agencies, individuals, foundations, corporations, and governments in the region.

Over more than fifty years of serving as a U.S.-based institution for public diplomacy in the Asia Pacific region with international governance, staffing, students, and participants, the Center has built a worldwide network of 65,000 alumni and more than 1,100 partner organisations. The Center's 21-acre Honolulu campus, adjacent to the University of Hawai'i at Mānoa, is located midway between Asia and the U.S. mainland and features research, residential, and international conference facilities. The Center's Washington, D.C., office focuses on preparing the United States for an era of growing Asia Pacific prominence.

WSD **HANDA** CENTER
FOR HUMAN RIGHTS & INTERNATIONAL JUSTICE
Stanford University

About the WSD Handa Center for Human Rights and International Justice, Stanford University

The WSD Handa Center for Human Rights and International Justice at Stanford University equips a new generation of leaders with the knowledge and skills necessary to protect and promote human rights and dignity for all. Reflecting a deep commitment to international justice and the rule of law, the Center collaborates with partners across Stanford University and beyond on innovative programs that foster critical inquiry in the classroom and in the world.

The Center pursues its mission through a range of international programs including justice sector capacity-building initiatives, civil society outreach efforts, trial monitoring, expert consultancies, and archival resource development, with a focus on transitional justice initiatives and new technologies.

The Handa Center operates globally, with international partnerships reaching particularly deep into Southeast Asia. Our overseas programs and partnerships focus on major global issues such as migration and human trafficking, accountability and peacebuilding in post-conflict societies, gender-based violence, freedom of religion and expression, corruption and the rule of law, and atrocity prevention. The Center also partners with the Stanford University Libraries to implement cutting edge justice sector and human rights archival resource projects in developing countries and elsewhere, with a focus on new technologies.

The Center invites student participation in the full range of our research and overseas programs, as an integral part of their academic experience. The Handa Center enhances Stanford's academic offerings and student opportunities by integrating classroom curricula with faculty research, funding student internships, facilitating innovative interdisciplinary collaboration, offering invaluable professional mentorship, and providing unique opportunities for fieldwork.

About the Author

Jessie Brunner serves as Program Manager of the WSD Handa Center for Human Rights and International Justice at Stanford University. Here she manages student programs, including the new Minor in Human Rights, as well as Center collaborations and several research activities. In addition to work on criminal justice reform, Jessie currently researches issues relevant to data in the human trafficking field, with a focus on Southeast Asia. She works on these issues at the local level as a member of the San Francisco Mayor's Task Force on Anti-Human Trafficking and at the global level as a member of Knowledge Platform Reference Group of Alliance 8.7, which helps set the UN agenda on Sustainable Development Goal 8.7 related to human trafficking and forced labor. Jessie is the author of *Inaccurate Numbers, Inadequate Policies: Enhancing Data to Evaluate the Prevalence of Human Trafficking in ASEAN* (2015), which she presented at the 8th Annual Summer Institute in International Humanitarian Law and Human Rights in Bali, Indonesia.

Previously, Jessie served as a researcher at the Center on Democracy, Development, and the Rule of Law's Program on Human Rights; a Public Affairs Assistant at the State Department in the Bureau on Democracy, Human Rights and Labor; a reporter for *Los Angeles Times* Community News; and a non-profit public relations/marketing manager. In addition to serving as a trial monitor at the Extraordinary Chambers in the Courts of Cambodia, Jessie has worked on human rights and post-conflict reconciliation in Argentina, Bosnia and Herzegovina, Brazil, Chile, Cambodia, Indonesia, Rwanda, the Philippines, and Thailand. Brunner earned a MA in International Policy Studies from Stanford University and graduated with Highest Distinction from UC Berkeley with a BA in Mass Communications and a Spanish minor.

GETTING TO GOOD
HUMAN TRAFFICKING DATA

Everyday Guidelines
for Frontline Practitioners
in Southeast Asia

British Embassy Jakarta
WSD HANDA CENTER FOR HUMAN RIGHTS & INTERNATIONAL JUSTICE Stanford University
EAST-WEST CENTER COLLABORATION • EXPERTISE • LEADERSHIP
HUMAN RIGHTS RESOURCE CENTRE