PRACTICE NOTE 8

CASE MANAGEMENT & DIGITAL SECURITY FOR STRATEGIC LITIGATION AGAINST TORTURE

December 2022

REDRESS
Ending torture, seeking justice for survivors

This guide is part of a series of Practice Notes designed to support holistic strategic litigation on behalf of torture survivors. It is aimed at lawyers and activists who assist torture survivors in the litigation process. This Practice Note explains the key building blocks of effective case management and digital security in the context of torture and ill-treatment cases. It makes suggestions based on consultations with NGOs, research reports, and practical experience. It will be useful for those new to strategic litigation to find out more about building effective case management techniques, and also for more experienced practitioners, to encourage reflection on how cases are managed and build on best practices.

REDRESS recognises that individuals who have been subjected to torture may choose to identify with the term victim, whilst others feel more represented by the term survivor. Whilst we respect everyone's choice to identify as they wish, throughout this Practice Note we will be referring to people with lived experience of torture as survivors, to highlight their resilience.

REDRESS would like to thank the **United Nations Voluntary Fund for Victims of Torture** and the **Matrix Causes Fund** for their generous support of this project. This publication was prepared by a team at REDRESS, including **Rupert Skilbeck**, Director, **Alejandra Vicente**, Head of Law, **Peace Amito**, Programme Manager, **Holly Huxtable**, Legal Officer, and **Eva Sanchis**, Head of Communications. We would like to also thank **Ely Cossio** and **Blánaid Ní Chearnaigh**, former REDRESS legal fellows, for their contributions to preparing this Practice Note. We are also grateful for the input offered by other NGOs conducting strategic litigation from LATAM, Africa, and Asia. REDRESS bears sole responsibility for any errors in this Practice Note.

REDRESS
Ending torture, seeking justice for survivors

CONTENTS

ANNEXES 44

INTRODUCTION

Strategic litigation allows human rights lawyers to challenge both the individual acts of torture and ill-treatment and the policies and practices that enabled it to take place. Legal claims can allow survivors to obtain accountability and other reparations, as well as to campaign for policy and legal reform to make it more difficult for torture and ill-treatment to occur in the future. Strategic litigation is often a highly complex task involving many moving pieces beyond the legal case itself, such as advocacy (national, regional, and international), activism, and engagement with the media, academia, and the wider public in general. Typically, these cases will span several years adding further complexity to ensure continuity of representation, active and ongoing consent, and regular holistic support to survivors.

Many anti-torture NGOs have large numbers of cases and must operate a case management system to organise their documents and keep track of deadlines and next steps in litigation. Some NGOs use paper-based files, which carry particular risks of damage or seizure. While electronic filing systems can mitigate this risk, they can be difficult to set up and are capable of being hacked by governments implicated in the case. Further complicating matters, different jurisdictions will have certain rules about storing and sharing sensitive data.

Inadequate case management creates real risks for NGOs engaged in anti-torture work and can jeopardise the safety of survivors, witnesses, and others involved in litigation. Slack systems make it easier for documents to be seized or interfered with, either physically or digitally. Poor professional standards may lead to disciplinary action, or sub-standard representation of clients where deadlines are missed. This may mean that the rights of survivors of torture are not protected and may also have a detrimental effect on the reputation and efficacy of the anti-torture movement.

Robust and secure case management systems enable organisations – particularly those with a large case load – to both organise and keep track of cases, while ensuring that the needs of survivors are provided for and that the strategic goals of the case are managed and met. Using checklists and developing streamlined processes for managing strategic litigation cases can have a direct positive impact on the outcome of a case and can help ensure that cases are dealt with fairly and effectively.

Yet, the contexts in which organisations work are wide and varied, each presenting their own challenges ranging from security to resource issues. While there is no "one size fits all" solution to effective case management, some basic principles can be put in place to foster the smooth running of a case, facilitate ongoing reflection and evaluation, and place the survivor's needs at the centre of the case.

This Practice Note highlights some good practices for case management in the context of torture and ill-treatment. Key principles are highlighted in bullet points at the beginning of each section. The text then goes on to detail activities and processes that can be put in place over time to strengthen strategic litigation. The Practice Note covers the following basic building blocks of effective case management:

a) Competent and Ethical Representation
b) Case Enquiries
c) New Cases
d) Document Management
e) Communicating with Survivors and Managing Correspondence
f) Managing and Collecting Evidence
g) Case Log and Litigation Calendars
h) Closing a Case

The Practice Note also covers the following general principles for digital security for effective case management:

a) Outlining and Understanding Risk
b) Safe and Sensitive Document Management and Disposal
c) Safe Communication and Information Sharing
d) Compliance

THE BUILDING BLOCKS OF EFFECTIVE CASE MANAGEMENT

A. Competent and Ethical Representation

- Survivors' representatives, whether legal and non-legal staff, must not disclose information related to the survivor's case, except if their consent is provided or if required to carry out the representation.
- The consent of the survivor must be obtained for all activities surrounding litigation. For example, consent must be sought not only for legal representation but also for media or advocacy campaigns. If the survivor decides not to proceed with the case, or wants to withdraw from the case, their wishes must be respected.
- Representatives should ensure that survivors are not harmed or retraumatised during the process of strategic litigation. Survivors should have access to ongoing support to cover their psychological, medical, or social needs.
- When starting a new case, representatives should plan, discuss, and agree the strategy of the case together with the survivor and any co-litigant organisations.

Throughout the life cycle of a case, representatives must offer competent and ethical representation. The role of a lawyer is to advise survivors on their legal rights and obligations, and on the legal procedures relevant to the litigation goals set by the survivor. Lawyers must assist survivors in every appropriate way and take legal action to protect their interests. Lawyers must also seek to uphold human rights and fundamental freedoms recognised by national and international law, and act freely and diligently in accordance with the law and recognised standards and ethics of the legal profession in their jurisdiction.

Non-lawyers are often involved in the representation of survivors. Non-lawyers and NGO organisations may bring cases on behalf of survivors before the UN individual complaints mechanisms as well as before regional human rights bodies. In these cases, there is often no specific external regulatory framework governing their actions – a factor which is relevant to potential negligence claims as well as discussions of confidentiality and legal privilege. Key elements of competent and ethical representation include maintaining confidentiality, obtaining informed consent, and the principles of 'do no harm'.

Confidentiality

Representatives working with survivors of torture and other grave violations deal with very sensitive information. As a result, those representing survivors need to be aware of their duties relating to confidentiality so that they treat information adequately and in compliance with data protection laws in their jurisdictions. While professional rules on confidentiality vary, generally lawyers representing survivors must not disclose information related to the survivor's case. Further, their ability to disclose information related to the representation is often limited to situations in which the survivor consents to information being shared, or where disclosure is required or permitted by law or implicitly allowed in order to carry out the representation. Generally, confidential information does not include 1) a lawyer's legal knowledge or legal research, or 2) information that is generally known or in the public domain.

Communications between a lawyer and a survivor are generally subject to legal privilege. Privilege protects communications (either written or oral) from having to be produced to a third party or a court. Legal privilege covers communications between lawyers and their clients made for the purpose of seeking or giving legal advice. Litigation privilege covers communications between lawyers and their clients in connection with actual or pending or contemplated litigation. The scope of this privilege varies by jurisdiction and may sometimes extend to a broader legal team. Where survivors are being represented by non-lawyers, it important to be aware that communications are unlikely to have legal privilege.

Particular care should be taken over sensitive information such as contact details, addresses, and personal data concerning health, sex life or sexual orientation, and personal data revealing any of the following: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership or other affiliations; genetic data; biometric data (where used for identification purposes).

Organisations must ensure that confidential information in relation to a case is not disclosed inadvertently and that everyone in the organisation, no matter their role, complies with confidentiality and the obligations it entails.

A potential breach of confidentiality must be dealt with immediately and it is prudent to put in place a standard procedure to be followed in case of a breach. If a determination is made that the incident could amount to a disclosure of confidential information, steps should be taken to:

a) assess the risk posed by the disclosure to people's rights and freedoms;
b) inform survivors of the potential risk due to disclosure;
c) mitigate any potential risks (i.e., taking information down from the website or the public domain); and
d) assess whether any other additional measures need to be taken to comply with the interest of the survivor and any data protection regulations.

Finally, representatives must keep information secure to avoid any potential hacking or security breaches that would compromise the security of the survivor and the integrity of the legal process.

Consent

The consent of the survivor must be obtained not only in relation to the legal representation but also in respect of the broader number of activities often associated with strategic litigation. For example, a survivor should consent to their identity being made public, to information about their case being shared with the media for advocacy purposes, and to information being disclosed to funders. The extended length of strategic litigation cases requires active and ongoing consent from survivors throughout the process of litigation. This could involve renewing

and obtaining renewed consent at regular intervals. (For more detail on obtaining consent, see *Section C: New Cases, Obtaining relevant consent for representation and advocacy*).

Do no harm

Representatives should ensure that survivors are not harmed or retraumatised during the legal proceedings or the search for justice. If the survivor decides not to proceed with the case, or expresses a desire to withdraw the case, their wishes must be respected.

Those working with torture victims should be aware of the impact of trauma and take measures to ensure that all interactions with survivors are sensitive to this. For more information on the psychological aspects of working with adult and child victims of trauma in strategic litigation, see *Module 13: Working with survivors of trauma.*

Similarly, representatives should be aware of the risk of vicarious trauma for staff members that are regularly exposed to distressing or graphic material or stories. Steps should be taken to ensure that staff have the necessary professional support made available to them if needed.

Holistic approach

A holistic approach to strategic litigation puts the survivor's needs at the core of the legal claim and advocacy strategy and requires that needs are assessed and met throughout the life cycle of a case. Survivors must have access to ongoing support to cover their psychological, medical, or social needs (for more information, see *Practice Note on Holistic Strategic Litigation against Torture*). Providing for these needs demands that they are considered and costed throughout the cycle of a case. This will often require collaborating with NGOs who specialise in providing such support to survivors of torture and ill-treatment from the outset of a case. Regular reflections of a survivor's needs and required referrals can and should be built into the case management process at regular intervals.

Building a Case Strategy

Holistic strategic litigation involves careful planning to ensure the case provides justice to the survivor and achieves as much impact as possible (see *Practice note on Evaluating the Impact of Strategic Litigation against Torture*). When starting a new case, representatives should plan, discuss, and agree the strategy of the case together with the survivor and any co-litigant organisations. A checklist can be used to consider the overall strategy of the case, the applicable law and preferred forum to litigate the case, the advocacy required to strengthen the impact of litigation, funding needs, risks and safety concerns involved, and other considerations. The strategy must be discussed and agreed with the survivor and any co-litigating partners and/or lawyers. A sample checklist can be found in Annex A.

B. Case Enquiries

- A central register where details of case enquiries can be logged and tracked is a useful organisational tool. Developing a process through which potential new cases can be reviewed and assessed can help organisations determine whether the case fits within their mandate and expertise, resource capabilities and, most importantly, with the objectives of the survivor.
- If the case does not fit the organisation's mandate, or it is decided that pursuing a case would not be in the best interest of the survivor, this information should be adequately communicated to the survivor as soon as possible. When possible, referrals should be made to other organisations capable of supporting the survivor's needs.

Most organisations receive case enquiries through websites, via telephone, in person requests, or through referrals from partners and other organisations. Depending on the number of enquiries received, handling new enquiries can be a time and resource intensive task. This is a crucial stage in the process of strategic

litigation and a pivotal one for survivors as it may be the first time that they are seeking assistance or sharing their story.

NGOs can designate one individual within an organisation to oversee and track all new enquiries. A central register where details of enquiries can be logged and tracked is a useful tool to enable an organisation to respond effectively. It can also assist in monitoring trends in the types of inquiries over time, which may provide useful information to the organisation and the anti-torture movement as a whole.

At the time of the first enquiry, the following information could be collected from survivors:

a) Name, address and contact details;
b) How they prefer to be contacted (e.g., via telephone or email);
c) Languages spoken and whether they require interpretation; and
d) Facts alleged: a short description of torture, when are where it occurred, by whom (names of authorities or individuals), and what happened.

Once a decision is made to represent a survivor, more information could be collected including:

a) Personal details such as gender, date of birth, nationality, current location, and residential status;
b) Brief details of any action already undertaken to seek justice, accountability, and reparation in the State where the torture occurred, in their home State or elsewhere;
c) Brief details of any remedies, reparations, or awards already made, if applicable, in the State where the torture occurred;
d) Brief details of any medical or psychological reports obtained relating to torture; and
e) Brief details of any other documentation of the torture available (photographs, witness statements or a list of people willing to provide statements; links to YouTube or other online videos; links to reports by NGOs or other bodies referring to the case).

How this information is collected will vary by organisation. Some organisations may require survivors to fill out a form on the website or collect this information in person or over the phone when they first make contact with the survivor. Having a full picture of the case very early on can assist representatives and organisations to quickly determine whether they are able to assist a survivor.

Organisations often have limited financial and human resources and therefore might not be able to take on every case they are presented with, even if they have the specific expertise to assist. Developing a process through which potential new cases can be reviewed and assessed can help organisations determine whether the case fits within their mandate and strategy, their expertise, resource capabilities, and, most importantly, with the objectives of the survivor.

Adopting a uniform set of criteria against which all case enquiries can be assessed may help to streamline the process and ensure that the case selection process is conducted fairly and in line with the organisation's mandate. Using a checklist to guide this process can serve to facilitate decision making. A sample checklist is included in Annex B.

If the case does not fit the organisations mandate, or it is decided that pursuing a case would not be in the best interest of the survivor, this information should be communicated to the survivor as soon as possible. Depending on the jurisdiction in which you are operating, it may also be necessary to delete all information in relation to the enquiry in compliance with general data protection rules.

If the survivor's case cannot be taken by your organisation, you may decide to refer them to other organisations that may be able to assist. For example, survivors could be pointed to another human rights organisation, to a lawyer, therapist, or support group.

C. New Cases

- A holistic assessment of the survivor's needs should be conducted as soon as an organisation comes into contact with the survivor.
- An organisation's legal procedures and obligations, as well as what is expected of the survivor should be clearly understood. Clarifying this early on can prevent future misunderstandings or conflicts.

Once a decision has been made to represent a survivor, the intake process begins. Through this process, the survivor should receive all the necessary information they need, and the scope and parameters of representation should be agreed.

Assigning a Staff Member to the Case

It is good practice to assign a single staff member to a case early on. This individual will be responsible for overseeing the case, tracking relevant deadlines, and being the point of contact for the survivor. While many individuals may eventually work on the case, assigning one point of contact allows a survivor to build trust and rapport with their representative.

Conducting a Holistic Assessment of the Survivor's Needs

Conduct a holistic assessment of the survivor's needs as soon as representatives come into contact with the survivor. This assessment should consider any medical, social, and psychological support needs that a victim may have. There is no "one size fits all" approach to conducting this kind of assessment and its scope might depend on the capacity of the organisation to respond to the client's needs.

Some organisations may choose to use a questionnaire or form to help guide the assessment. This approach is particularly useful when assessments are conducted by those without specialised training on the impact of torture on victims, as it may help to ensure survivors' needs are not overlooked. Alternatively, an unscripted conversation guided by a professional who is aware of the specific impacts of torture on survivors will often lead to a better outcome and can be less formal for the survivor.

These needs should be recorded so that they can be reassessed throughout the life cycle of a case. Annex C includes a sample form that could be used to record the results of an individual needs assessment. Ideally, a holistic assessment could be conducted before a final decision is made to take forward a legal claim, so as to ensure the survivor can make an informed decision as to whether it is in their best interests to do so.

The spectrum of needs of torture survivors is wide and varied, and often the organisation or individual taking care of the legal case will not be equipped to deal with psycho-social support needs, for example. As a result, developing strong referral pathways to ensure specialised support that can meet those needs is key. Referrals should be prompt and direct where possible to avoid a situation where a victim is bounced between support providers.

Organisations and advocates can keep an up-to-date list of organisations or individuals providing specialised support to torture survivors to facilitate quick referrals. Organisations could also consider making this information available to survivors in an accessible manner so that they may self-refer should they choose to.

While it is critical that the survivor's needs are assessed at the outset of any engagement with them, a holistic approach to strategic litigation requires that needs are assessed *continually* throughout the litigation process. A survivor's needs will often not remain the same throughout the lifetime of a case, particularly a case that spans a number of years, and it is the job of the survivor's advocate or representative to respond to any changes and organise relevant support accordingly.

Client Care Letters

In any intake process, the basis upon which an organisation will carry out the work on a case should be agreed upon from the outset. An organisation's legal procedures and obligations, as well as what is expected of the survivor, should be clearly understood. Doing this early on can prevent future misunderstandings or conflicts.

Clients may find it useful to have this information written down so that they can refer to it later. A "client care letter" is a useful tool for presenting key information

to a survivor. Such a letter could cover:

- Information about your organisation;
- How representatives will manage the survivor's case;
- The contact details of the person responsible for the work, where they are qualified and who they are regulated by (note this may not be relevant where survivors are being represented by non-lawyers);
- Information about preferred methods of communication. For example, if a survivor has expressed concern about email safety, this may include information on how secure communications will be ensured throughout the case;
- A summary of the survivor's instructions regarding their case;
- A list of actions for the survivor to take (e.g., to send relevant documentation);
- A list of actions that you will take;
- Agreed next steps;
- Any confidentiality clauses;
- How data, information, and documents will be held;
- Time scales;
- Publicity; and
- Complaints.

See Annex D for a template client care letter that can be quickly adapted to various contexts and cases.

The letter should also provide survivors with detailed information about the services you offer and what it may cost. Although most strategic litigation work is conducted *pro-bono*, it is important to discuss any costs that may arise throughout the litigation process with clients (for example, trips to attend hearings, the production of evidence, etc.) and whether those costs will be covered and how. Other issues that organisations might want to include, depending on their jurisdiction and needs, are details on their professional insurance related to casework, confidentiality, and data protection. All information should be presented in a user-friendly manner and in a language that the client understands.

Obtaining relevant consent for representation and related advocacy

Where representatives work on a case within an organisation it is important to obtain the survivor's consent for the organisation to act on their behalf. This allows the organisation to continue representing the survivor, even if the individual staff member assigned to the case leaves the organisation. Often survivors will be asked to sign an "Authority to Act Form" which will authorise one or several lawyers or other representatives within the organisation to act on behalf of that survivor and will describe the scope of the legal representation. This authorisation can also provide consent for lawyers or their organisation to provide information about the case to funders and others. A sample consent form is found in Annex E.

While consent from the survivor is required in most cases to initiate a legal claim, there are exceptions to the rule. In some cases, victimisation of a survivor may be ongoing; for example, a survivor may still be in incommunicado detention without access to lawyers; legal action might be needed in relation to an unidentified group of victims who are at imminent risk of torture (i.e., a group of migrants); or the special situation of vulnerability of the survivor does not allow representatives to get consent (i.e., victim in a psychiatric institution). In these cases, obtaining consent can be difficult, and it is usually not required by regional and international human rights bodies and courts.

Work undertaken beyond litigation may also require separate consent forms. For example, if an organisation is launching a media campaign around a case, then a separate consent form for communications work is a good idea. Often staff will also need access to documents related to the case that are held by a third party such as a partner organisation or another lawyer. In these cases, the staff member may also ask survivors to sign a specific form for the purpose of authorising the organisation to seek documents from third parties.

Often strategic litigation spans jurisdictions and organisations, and therefore organisations will seek the assistance of a local lawyer, organisation, or *pro bono* law firm to represent a survivor directly in a specific national or international jurisdiction.

This might be the case, for example, if the organisation relies on a national lawyer to help the survivor exhaust domestic remedies in their jurisdiction. In such instances, it is advised that the organisation and local lawyer representing the client in the national jurisdiction sign a "Partnership Agreement", stating the responsibilities and scope of representation of the third party, as well as any issues related to legal fees and costs, deliverables, and other points relevant to representation.

Collecting and logging all relevant documents

All documents on a case should be carefully filed at the outset of a case. Recording a summary of a document, where it is located, and its significance at an early stage will help indicate where there may be gaps in evidence and serves to avoid any doubt as to the provenance and relevance of a document at a later stage. This process can be repeated at a later stage when building and collecting further evidence. A simple template can be found in Annex F. All documents should be saved electronically, and any original documents can be kept in hard copy (see *Section D: Document Management*).

D. Document Management

- Representatives working on torture cases should establish effective systems for document management. It is helpful to have a file management structure that is uniform across the organisation to allow current and future staff to navigate and locate files easily.
- Some organisations may use online case management or cloud-based storage tools to assist with document management. When selecting these tools, efforts must be taken to ensure they meet the necessary security requirements.

Representatives must represent torture survivors competently, which includes ensuring that they meet deadlines and that they look after documents. The same ethical obligations apply to NGOs representing survivors. This requires representatives to maintain effective systems for document management. While organisations may have different resources available to them, simple measures can be implemented for document management to facilitate better organisation:

Using technology

Some representatives may use online case management or cloud-based storage tools to assist with document management and storage. When selecting these tools, make sure they meet the necessary security requirements.

Paper-based filing systems

While many representatives have moved online, others continue to work entirely or partly on paper which may leave them more vulnerable to searches and seizure of sensitive documents by the authorities. If possible, it is important to ensure that representatives have an electronic copy of all documents so that files are not lost in the case of possible confiscation of documents through raids, seizures, or any other potential damage.

Setting up folders and subfolders for each case

It is helpful to have a file management structure that is uniform across the organisation that allows current and future members of staff to navigate and locate files easily. Where cases may span several years, organised filing systems allow for the case to be easily passed between staff. Files could be organised by type of document, by stage of the proceedings or using a different system as long as it is uniform and effective. For example, case folders could contain the following subfolders:

- **Admin** (containing contracts, legal representation agreements, powers of attorney, client care forms etc.);
- **Background documents** (containing background information on domestic proceedings, research documents, media reports, other NGO documents, country reports);

- **Evidence** (containing all supporting documentary evidence that has been, or will be, submitted in the case. It includes correspondence that is used to prove exhaustion of domestic remedies or another aspect of the case and numbered evidence for submissions in sub-folders);
- **Correspondence** (containing litigation correspondence, which includes external correspondence by mail, fax, and email to and from courts, States and national authorities, partners, third parties and others. It also includes relevant internal correspondence (email). All correspondence that is also used as evidence should be copied in the evidence folder);
- **Submissions** (containing main legal documents for filing in a case, as well as any pleadings in response. It could also include outlines of arguments and drafts. If a case has been submitted to several jurisdictions (national, regional, etc.), subfolders could be created for each proceeding (i.e., Kenya, ACHPR));
- **Decisions** (containing any decisions issued in the case, including precautionary measures, interlocutory decisions, final decisions and judgments, and implementation); and
- **Implementation** (containing any submission, decision, correspondence, and others related to the implementation of the decisions in the case).

Establishing a naming convention for documents

Organisations can agree on naming conventions when saving documents electronically to enable files to be more easily located by representatives working on the case. This may include elements such as:

- *Date.* Usually, the date that the document was created.
- *Case Name.* Use the family name of the client/applicant, or an NGO.
- *Short Title.* A specific and concise description that identifies the document.
- *Author.* It is very helpful to know who produced the document. If the document is produced by a staff member/caseworker, you could use the

initials of that staff member. If the document is a court or State produced document, you could use the acronym or short name of the court or UN body.

- *Multiple Drafts.* Where a document undergoes multiple drafts, it is useful to save the document with the latest date. That way, if there are multiple drafts it is very easy to find the latest draft, by searching for the latest dates. Avoid using "FINAL DRAFT", "VERSION C", "MY LATEST VERSION", "USE THIS ONE".

Maintaining copies of documents filed with courts or judicial bodies

It is good practice to keep both word versions, pdf versions with signatures and a public version (with sensitive information redacted of documents filed in courts or judicial bodies, if necessary).

Translations

Where two versions of the same document exist in different languages, it is useful to indicate the language as a suffix, using exactly the same title. This way the two electronic documents appear side by side in the folder.

Regular review of documents

Representatives should regularly review documents in a case file to ensure that all documents are saved correctly and there is nothing missing in the case file. A table can be used to track significant documents. An example is found in Annex F.

E. Communicating with Survivors and Managing Correspondence

- All communications should be conducted safely and securely.
- Contact with survivors should be maintained throughout a case, even during periods of inactivity.
- Representatives should keep a record of all communications with survivors, particularly where advice or instruction given, or strategy is discussed with partners or other lawyers.

All communications with a survivor should be conducted safely and securely. If there are heightened security risks, then both the means and storage of communications should be adapted (see *Digital Security for Effective Case Management).* In some cases, representatives may not have direct contact with a survivor, and communication may be through partner organisations for example. In these cases, representatives should ensure that their partners are maintaining regular contact.

During a case there are often long periods of time – sometimes many years – in which a case is inactive or dormant. During these periods, it is important to ensure that contact with survivors is maintained. This can avoid situations where a case becomes active again at short notice but communication with a client has been lost. Keeping regular contact also ensures that active consent to participate in a case is regularly updated and maintained.

Communication in person or over the phone

Communication with survivors throughout a case may take many forms, and range in frequency. Whether speaking in person, over the phone, or via email, keep a record of these communications – particularly in instances where advice or instruction is being given, or strategy is being discussed with partners or other lawyers. These records can prove invaluable to clarify and resolve queries in the future.

For communication that takes place in person or over the phone, meeting notes can be taken to briefly summarise the communication and any action agreed upon. Developing a template for attendance notes can help facilitate this process.

Correspondence via email

Recording and tracking communications via email can present challenges, particularly where multiple individuals may be working on a case. Some of these challenges have been overcome by cloud-based systems that allow for automatic filing of emails. However, even where automated systems do not exist, copy all email communications to the case file to keep an accurate record.

Correspondence via post

Where correspondence is via post, all letters received in hard copy should be scanned and saved in the electronic case file. Maintaining a scanned copy will often suffice and the original letter may be discarded, unless the original document is not replaceable, as with a notarised affidavit or a stamped court document. These can be kept in the hard copy case file.

Correspondence with courts and tribunals

Most substantive correspondence with international, regional, or UN bodies should be sent in a formal letter which can be sent electronically by email (attached as a PDF with a brief description in the body of the email). Documents should be sent in accordance with the rules of procedure of the relevant court or human rights body. For example, correspondence with the European Court of Human Rights (ECtHR) requires a barcode, provided by the court when the case is registered, be placed at the right-hand corner of the first page of all letters. However, once the case is "communicated" to the relevant State, all communications should be sent through the ECtHR electronic portal. The Inter-American Commission on Human Rights (IACHR) also processes cases through a case portal. Both the IACHR and the Inter-American Court of Human Rights accept electronic files as long as the documents contain an electronic signature.

Other courts and bodies still require the electronic copy by email, accompanied by a hard copy of the document sent by regular mail. While this was the case with the African Commission on Human and People's Rights (ACHPR), the Commission now accepts documents in electronic version only (sent by email). Review the relevant court's practice directions for any specific format requirements for correspondence and written pleadings.

When sending a document to the court or survivor, keep some proof that the document has been sent. For example, keep a copy of the email in the electronic case folder. Or, if you send a document by regular mail, you can ask for a certificate of mailing from the post office. Where documents are faxed, the sending report could be attached to the document in the relevant file and saved in the electronic case folder.

F. Managing and Collecting Evidence

- When conducting interviews for victim or witness statements, representatives should bear in mind that survivors are being asked to recount highly traumatic events and interviewers must take necessary precautions to avoid retraumatisation.
- It is critical that the logistical issues associated with building an evidentiary base and taking witness statements are taken into account early on in the case management process, including budgeting for consultants when needed, and establishing secure information sharing processes amongst partners.
- All evidence must be properly named and filed in an agreed location or folder.
- In some contexts, collecting or storing evidence may present security risks for both the survivor and representatives. These risks should be evaluated and addressed, and mitigation measures should be adopted when possible.

Sources of evidence in a torture case may include victim statements, statements from witnesses, expert reports, physical and forensic evidence, UN, and NGO reports documenting patterns of violence, and various forms of media, including newspapers and secondary sources. What is needed will depend on the type of proceeding and the burden of proof required (see *Practice Note on Holistic Strategic Litigation Against Torture*). Often collection of evidence will involve a number of partners, such as international and national lawyers or international or national NGOs.

When documenting cases of torture and ill-treatment, there is useful guidance in the Istanbul Protocol and the International Protocol on the Documentation and Investigation of Sexual Violence in Conflict (FCO Protocol) (see *Practice Note on Istanbul Protocol Medico-Legal Reports,* and *Module 15: Evidence of Torture).*

When conducting interviews for victim or witness statements, representatives must bear in mind that survivors are being asked to recount highly traumatic events and interviewers must take necessary precautions to avoid retraumatisation. When conducting interviews, the following should be taken into account:

a) **Preparation.** What is the purpose of the interview? What is the information you are seeking to obtain? Usually, the primary objective of an interview is to collect evidence to show that person was tortured, to build support for the legal elements of torture, and that the alleged perpetrator is responsible for the offence. Keep in mind the need for consistency and detail. The needs of the survivor should be the central consideration.

b) **Logistics.** Interviewees should feel comfortable and safe. Representatives should provide the following: a safe location, note-taking method, food, drinks, ability to take breaks etc. Survivors should also be given the option to choose the gender of the interviewer. This is particularly important in cases concerning survivors of SGBV, where specialist advice should be sought.

c) **Language.** If the interviewee does not speak or understand the same language as the representatives, they will need an interpreter, which requires advance planning and budgeting.

d) **Confidentiality.** It is the obligation of representatives to explain to the interviewee the issue of confidentiality, the manner in which their statement be used, and how they will be protected.

e) **Location.** Consider the room, its layout and the people present. Will the interviewee feel safe and at ease?

f) **Recording and storage.** If representatives decide to record the interview, the interviewee's consent must be sought first. Representatives must ensure they have the means to safely store the data and explain these protocols to the interviewee.

g) **Special arrangements**. Certain survivors may require specialised support and consideration when conducting interviews. For example, survivors

of SGBV, or child survivors. In these cases, interviewers need to have the requisite knowledge and skill to conduct interviews. For more information, see *Practice Note on Working with Child Victims of Trauma* and *Module 4: SGBV as Torture*.

h) **Other considerations.** Representatives must think about other issues that may be important when interviewing a survivor or witness of torture: how will trauma impact the interviewee? Should a medical or psychological support person be present? Is there a fear of reprisal if the person speaks with representatives? How can you ensure the safety of the person? What precautions can be taken to minimise the fear of reprisal? If the victim has children, can childcare be provided during the interview?

All evidence must be properly named and filed in the case folder. If the evidence is in a language other than the language in which the submission is being drafted, the documents might need to be translated.

In some contexts, collecting or storing evidence may present security risks for both the survivor and those collecting and storing the evidence. In these cases, the security risks should be evaluated and addressed, and mitigation measures adopted when possible.

G. Case Log and Litigation Calendars

- Use a case log to track significant movements in a case.
- Put in place tools to ensure that legal deadlines are complied with.

In addition to saving documents and recording communications, you can track significant movements in a case using a Case Log. The log must be regularly updated and can include information on the individual representatives working on the case, contact information of the survivors, background information on the case, violations/crimes, submissions made, actions taken, and next steps planned. Online

tools can be used to assist with this; something as simple as a regularly updated word document might serve the purpose. If a detailed and regularly updated case log is maintained, the impact of staff turnover during the long period of a case will be less significant, allowing for large caseloads to be managed more easily.

Recording and meeting deadlines is critical in human rights litigation as missing a deadline could have the result of depriving a survivor of their only chance to obtain justice, truth, and reparation. While the individual assigned to the case should have primary responsibility of recording and meeting deadlines, it is useful to record deadlines across cases in a shared calendar so that representatives have a clear overview of workload and can plan accordingly.

H. Closing a Case

- At the end of a case, documents should be returned to survivors or disposed of appropriately and in line with data regulation rules.

A casefile might need to be closed once representatives are satisfied that all issues relating to the case have been concluded and following a consultation with the survivor. If so, the case should be closed in a way that ensures all data and documents related to the case are handled in accordance with legal and ethical obligations, and in compliance with any applicable data regulation rules in the specific jurisdiction.

Closing a case, even when necessary, may have an impact on the survivor, particularly in cases where the survivors' expectations of the litigation outcome were not met. Clear and open communication is vital in this regard, as well as ensuring that survivors have continued access to psycho-social support after the litigation, if required.

When to close a case

NGOs will generally represent survivors until all issues related to the case have been concluded in a satisfactory way. However, the issue of whether to close a case may not be so clear cut.

In some situations, representatives may have agreed only to complete part of the litigation process, while in others a case may have reached an impasse and it may not be in the best interests of the survivor and representatives to continue it. When it is not possible to ensure that implementation of a decision in favour of the survivor is achieved in full, actively maintaining cases might raise the survivors' expectations that further steps can be taken where in reality such steps are extremely unlikely. Organisations may, therefore, wish to close cases in circumstances where the implementation phase is not fully satisfactory if a number of criteria are met. When considering whether to close a case of this kind, there should be a careful discussion with the survivor to review the options, and the criteria to be considered mirror those used as the beginning of a case and allow for careful consideration of whether limited resources can and should be used for ongoing work in the implementation of a case. A checklist containing criteria to be considered when closing a case can be found in Annex G.

Closing a Case

Once a decision has been taken to close a case, a letter can be sent to the survivor explaining the arrangements for storage and/or handling of their file. Electronic files should be kept. Hard copies can be destroyed if there are electronic copies, save that original documents should be kept. The length of time that documents must be stored may vary by jurisdiction. In some cases, representatives may wish to retain case documents indefinitely to have a historical record of the human rights violation that occurred.

Similarly, certain original documents may be valuable to the client and difficult to replace, e.g., medical records, deeds, birth certificates, death, or marriage certificates. Once a case has finished, it is important to return these to the client where possible, with a record of the return (e.g., a recorded delivery slip or signed receipt). Where these cannot be returned, they should be retained. It is often useful to use a checklist to ensure a consistent approach to case closure. A sample checklist is included in Annex H.

Destruction of any part of the file should never be automatic, even when the proposed destruction date is reached. Instead, the file should be checked by someone who appreciates the importance of the task; this is not simply an administrative task and consideration should be given to each file on an individual basis. A File Storage/Destruction record can be kept noting: the files stored, details of the provisional destruction, the date of destruction of any part of the file, the name of the person who authorised destruction, and the reason for destruction.

Most of the documents on a file belong to the client and, strictly speaking, should not be destroyed without the client's consent. In reality, it is often impossible to obtain consent at the time you are considering destroying files (or parts of them), so this should ideally be dealt with in the client care letters and/or file closing letter.

In situations where you do not have the client's consent to destroy the file (for example, cases which were finished many years ago), a balance will need to be struck between the ongoing cost of storing files and the risks attached to destroying them (e.g., that the client may want the file back or may bring a claim or complaint to this effect). In such cases, attempts should be made to contact the client giving them the opportunity to have the documents sent to them or to seek their permission to destroy them. If no response is received, a risk assessment can be conducted and, based on the results, a decision should be made to either retain the file for a further period, or to securely destroy the file (or part of it). Such an assessment should consider the following questions:

- Do representatives have consent to document destruction (in client care letter, or file closing letter or elsewhere)?
- Are there any original hard copy documents on the file? If "yes", these should generally be retained in any event.
- Is there anything on the file to suggest that a claim/complaint might yet be made?
- Has the primary limitation period in the representatives' jurisdiction expired in connection with any advice given in this matter?

- Are there any longer limitation periods likely to apply to any aspect of the client's problem (e.g., family case, partnership issue, property disputes)?
- Was this a complex case?
- Was the survivor vulnerable? Was communication challenging with this client?
- Is the survivor likely to instruct the same representatives again?
- Do representatives need to contact their insurers to seek advice before destroying the file?

In this event, original documents should generally be retained for the reasons set out above. Obligations under data protection legislation vary according to jurisdiction but may require representatives not to retain data or documents for longer than is necessary.

DIGITAL SECURITY FOR EFFECTIVE CASE MANAGEMENT

Many NGOs case management systems combine the use of paper based and electronic filing and systems for communicating. There are risks associated with either, so the measures taken to secure files and mitigate their risks are different. While the focus of this Practice Note is digital security, materials related to the physical protection of staff, office premises, and documents can be found in the further reading below.

People are the foundation of digital security. Security is a team effort and responsibility. When it comes to case management, NGOs should train and encourage all staff on data security knowledge. Putting in place effective digital security processes can take time and be resource intensive, so a step-by-step approach is helpful.

A. General Principles for Digital Security

- **Prevent.** To avert any potential hacking or security breach that would compromise the safety and rights of survivors, NGOs may choose to design and implement a data breach prevention plan to keep confidential data safe. A simple risk assessment can be undertaken to identify possible weaknesses.
- **Protect.** When using online tools, NGOs should ensure that these tools are provided and supported by trusted suppliers, configured to reduce the possibility of security breaches, and administered in a secure and accountable manner.
- **Respond.** Where there has been a data breach, NGOs must assess the type of data compromised by the breach, the person or number of persons

impacted, the potential harm to them as a result of the breach, and then implement a recovery plan to redress any damage.

These principles aim to provide strategic guidance on how NGOs can protect their systems and data from digital threats and safeguard survivors' human rights and fundamental freedoms, particularly their right to privacy.

Prevent

Compared to threats experienced in the physical world, digital threats can be harder to detect. This means that identifying, understanding, and preventing digital security risks is essential for good case management.

To prevent any potential hacking or security breach that would compromise the safety and rights of the victim, NGOs are advised to design and implement a data breach prevention plan to keep confidential data safe. This prevention plan should include how data will be protected, what to do if there is a breach, and how to mitigate the impact on survivors' privacy and security.

Training is an essential part of any prevention plan. NGOs should train their staff, especially those working on litigation, so that they are aware of digital threats and what they should not do or should avoid when working on a case.

Protect

Some NGOs may use online case management or cloud-based storage tools to assist with document management and storage. When choosing these tools, evaluate whether they meet the necessary security benchmarks for the type of work they are doing. NGOs should ensure that these tools are provided and supported by trusted suppliers, configured to reduce the possibility of security breaches, administered in a secure and accountable manner, and that security vulnerabilities can be identified promptly.

Respond

When a security incident takes place, NGOs must respond quickly to determine whether a personal data breach has occurred and, if so, take immediate action to remediate it. Once representatives become aware of the data breach, they should assess the type of data compromised by the breach, the person or number of persons impacted, the potential harm to them as a result of the breach and implement a recovery plan to redress any damage.

A data breach can compromise the security of a victim and violate their human rights and fundamental freedoms, including their right to privacy. It can also cause considerable damage to representatives and their reputation. This means that representatives should prepare their response to such a breach, with adequate policies, mechanisms, and procedures in place that can be followed.

In some countries, there may be an obligation to report such a breach to the data protection authorities, or to an NGO oversight body.

B. Outlining and Understanding Risk

Understanding and assessing risk is a crucial step to protect sensitive information and an essential component of the risk management strategy of NGOs. This requires a risk assessment to mitigate the risk of any security breach, cyberattack or data leak that may affect victims' rights and safety, as well as the organisation.

When assessing security risks NGOs should consider:

a) What is the NGO's most crucial information technology resources?

b) What type of data breach (whether from malware, cyber-attack, unauthorised access, or human error) would significantly impact the work of the NGO?

c) What is the source of the threat(s), if detectable, and the potential impact of each identified threat?

d) What level of risk is the NGO comfortable taking when dealing with sensitive

data and confidential information provided by survivors or victims of human rights violations?

Once these factors have been considered, NGOs can determine what it is they need to protect. These factors will also assist NGOs to better understand the value of the data that needs to be protected.

Digital risk assessments

While not all digital information can be protected, all digital data is vulnerable to being breached–hence the importance of performing a risk assessment. No single rule exists on how to complete a risk assessment; nevertheless, the following steps can provide some guidance on where to start and what to do.

a) **Identification.** NGOs should identify all the digital assets, that is, any file created electronically and that exists as data contained on a digital storage drive or computer, that may be exposed and vulnerable to unauthorised access, particularly those with sensitive information. Digital assets may include a survivor's contact information, sensitive documents, and electronic signatures. Once the assets are identified, organisations should create a risk profile for each of them, identifying possible threats and the sorts of security they correspondingly require. For example, if the identified asset is the victim's contact information and the possible threats are it getting stolen or accessed by an unauthorised person, the organisation could secure the assets by encrypting the file, adding a password, or limiting who can access it.

b) **Assessment.** Once a risk has been identified, it needs to be examined. Specifically, NGOs must assess the event's likelihood and the impact it would have on the case, the victim, and their organisation. This assessment helps define each risk's priority level and the measures needed to mitigate it. For example, if the risk is data theft by a malicious insider that would jeopardise a victim's privacy and the organisation's work, there are various measures that could be implemented to respond. This could include measures such

as installing antivirus software, using password protection, encrypting data, securing the organisation's Wi-Fi network, properly disposing of sensitive data, controlling access to devices and sensitive files, etc.

c) **Mitigation.** It is paramount to implement security measures and other steps to decrease the prospect, the possible impact, and the risk level of the threat. For example, NGOs can implement a crisis management plan, a data leak prevention strategy, or a cyber-attack prevention policy.

d) **Prevention and Monitoring.** Monitoring risks over time to remain on top of emerging security challenges is an effective preventive strategy. Representatives should also implement effective preventive safeguards that alert lawyers, caseworkers, and other professionals engaged in litigation and case management on how to prevent, detect, and respond to digital threats.

How to mitigate digital risk

Once representatives have identified digital risks and the impact these risks might have on their legal work, they should implement a plan to mitigate the risks. Possible mitigation strategies include:

- Adopt digital security policies to protect the organisation's work and the victims' personal data and information. For instance, representatives could adopt an information-data security policy, an incident response policy, a remote access policy, a risk management policy, and a fraud policy, among other policies.
- Change passwords regularly and implement strong authentication controls, such as two-factor authenticators and password managers.
- Use privacy-boosting browser extensions to avoid website visitor tracking.
- Make use of virtual private networks (VPNs) to connect to the Internet via an encrypted tunnel, thus preventing any data security threat.
- Install antivirus software and a firewall on the laptops or devices used by the

lawyer, caseworker, or any person involved in litigation who has access to and control of sensitive and confidential information.

- Run periodic penetration tests on the organisation's digital infrastructure.
- If possible, avoid connecting to public WIFI. If using public WiFi, being sure to log-out.
- Keep the software and operating system on computers updated.
- Carry out a risk assessment regularly.
- When digitally managing cases, secure all case folders, and limit access to essential personnel. Once a shared folder is created, administrators can restrict users' access by changing the folders' security permissions. Folders will remain public until the admins provide groups or individuals with access.
- When reading emails or messages in a chat, exercise caution when opening unexpected links or attachments.

C. Safe and Sensitive Document Management and Disposal

- Documents should only be retained for as long as the information is required for strategic litigation or by law. This helps to minimise risk. When it is determined that documents are no longer needed, they should be disposed of safely.

Securely managing and disposing of documents is crucial to prevent any leak of information or access to it by unauthorised people. An organisation should only retain sensitive documents and data for so long as the information is required for the specific purpose for which it is maintained or as required by relevant law. For example, when an organisation has closed a case, the organisation can dispose of the information (see *Closing a Case)*. If the NGO chooses to keep it, it cannot be beyond the time permitted by its internal policy or applicable law. It must be

safely stored to prevent the information from being accessed, handled, or used by unauthorised individuals.

When keeping sensitive documents and information, it is also recommended that NGOs implement a retention plan. This plan should specify the level of sensitivity of the documents, the reason the documents are retained, and, if not previously requested, the victim's consent for representatives to preserve the information. This plan should also include the length of retention, how the documents will be stored and secured, and the procedure for effective documents' disposal.

When documents are disposed of, representatives should keep a **record of their disposal**, including a description of the files, and date of destruction. It is the obligation of representatives to ensure that the procedures employed throughout the disposal process offer suitable protections against the unintentional loss or disclosure of the documents' contents. Shredding, for example, is one of the safest and most cost-effective methods to dispose of sensitive physical materials. When it comes to digital files, one of the most secure ways to destroy them is by hiring a certified IT company. Once the company has disposed of the files, it will issue a disposal certificate that provides proof that all confidential information has been securely destroyed. The certificate includes, among other things, the destruction date and a description of the destroyed files and data. When a certified IT company cannot be hired, representatives can install a secure deletion software to clear or overwrite digital information.

All representatives and other staff, particularly those authorised to access, handle, and use sensitive documents and data, must be trained on the policies, standards, and processes to manage, and dispose of sensitive documents securely.

D. Safe Communication and Information Sharing

- When sharing sensitive information with partners on a case, adopt safe communication and information-sharing measures to minimise the risk of adversaries having access to sensitive information. Enhanced security measures may be needed for information which jeopardises the safety of sources and their associates; endangers the safety of survivors, representatives, and others; refers to projects or litigation strategies which may be undermined if exposed; or which includes evidence that is not publicly available.

General Practice

Legal work might require sharing sensitive information with different parties involved in a case, including lawyers, survivors, judges, or any other person assisting. However, when representatives share data with others, their adversaries have a higher possibility of accessing it. Therefore, sensitive information should be shared using secure communications tools and strategies.

For safe communication and information sharing, NGOs can use the following measures:

- Add a confidentiality notice or disclaimer when sharing confidential information by email. This notice should stress that the information is for the exclusive use of the intended recipient(s) and that any distribution, copying, or unauthorised use of this communication or the information in it is strictly proscribed.
- Proceed with caution when accessing emails, links, or attachments from unfamiliar sources.
- Use encrypted platforms, such as Tresorit, Proton mail, or digital share systems, such as Office 365 sharing or Dropbox, to share documents. If documents contain sensitive information, they should be password protected to control access to the document.

- Implement an information-sharing agreement (ISA) when sharing sensitive documents and information with external parties. The ISA should contain, among other things, a context-specific data and information sensitivity categorisation, instructions on how the data might be used, the responsibilities of the involved parties, and a procedure to handle protocol breaches.

Enhanced Security Measures

Determining when enhanced security measures are necessary will rely on the representatives' discretion, but an "if in doubt, do" approach is recommended. Enhanced security measures may be needed for information which jeopardises the safety of sources and their associates, endangers the safety of survivors, staff and others working on a case, refers to projects or litigation strategies which may be undermined if exposed, or includes evidence that is not publicly available.

NGOs can implement any measure needed to enhance the security of their communications and information. For example, to increase the protection of communications and information, NGOs can:

- Use project code names when discussing or sharing information about the project with people outside their organisation;
- Use end-to-end encrypted email, encrypted file sharing, and encrypted messaging and voice apps such as Signal and Telegram;
- When using Zoom video conferencing, require a password to join sensitive meetings;
- When using WhatsApp for texting messages or sharing documents, check the 'contact info' page and activate the disappearing messages setting;
- Wherever possible, have face-to-face meetings. When sharing sensitive information, turn off mobile phones or leave them outside the meeting room;
- When travelling, clean the phone and laptop's desktop and recycling bin. If that is not possible, staff should travel with a phone and laptop with no

other information on them. Any laptop should be able to be remotely wiped by employing easily obtainable software;

- Protect sensitive documents by adding passwords;
- Provide printouts of documents instead of electronic versions whenever the security situation demands it;
- Use a Microsoft document inspector to remove metadata from documents when the author's safety is at risk;
- Use anonymous social media accounts for researching people of interest; or
- When researching information of interest, use 'incognito' / 'private browsing' to protect search history information and prevent use of cookies.

Preparing for and Managing Breaches

As a general rule, data should be secure against any threats and safely and appropriately disposed of when no longer needed or required by law or internal policies. In case of a security breach, NGOs should implement a strategy to mitigate the harm caused, assign responsibilities where appropriate, and provide access to redress and compensation when required. Confidentiality breaches should be promptly reported to the designated person within the NGO to determine whether the incident amounts to a disclosure of confidential information.

While making the determination, the 'responsible person' should assess the risk to people's rights and freedoms, including those of the survivor, take steps to mitigate any potential risks, and notify the survivor of the confidentiality breach. The notice should detail the nature of the breach, the repercussions to the victim's rights, and the steps taken or intended to be taken to minimise and remedy any negative effects.

E. Compliance

- Ensure that staff working on strategic litigation are aware of the obligations of data protection in their jurisdiction when they collect or handle data about an individual survivor.

In some jurisdictions, representatives must abide by regional and/or domestic legal standards concerning data protection and management. They must be aware of the local obligations of data protection when they collect or handle data concerning an individual. In the European Union, for example, the General Data Protection Regulation (GDPR) lays down rules regarding the processing and free movement of personal data. Accordingly, European organisations are required to collect and process personal data in accordance with their responsibilities under the GDPR. This requires NGOs operating in Europe to have in place a data protection policy.

FURTHER READING

- Workbook on Security, Frontline Defenders, **https://www.frontlinedefenders.org/en/workbook-security**
- Security in A Box Digital Protection Resources, Frontline Defenders, **https://www.frontlinedefenders.org/en/digital-protection-resources**
- The Holistic Security Toolkit, Open Briefing, **https://toolkit.openbriefing.org/the-toolkit**

ANNEX A
CASE STRATEGY CHECKLIST

OVERALL STRATEGY	**The problem** • What is the human rights problem the case is addressing? • What research do you have on the causes of the problem and potential solutions?
	Impact • What is the long-term goal the case seeks to achieve? • What does the case need to change to achieve that long-term goal? Law, policy, or practice? • Who has the power to change it?
	Coalitions • Which other organisations or individuals are working on this issue? • Who will you work with to address it?
	Strategy • How will litigation progress the broader strategy? • How will the decision be implemented, and by whom?
THE CASE	**Case Overview** • Explain the case in three sentences. • Who are the Claimant/s and the Defendant/s? • Summarise the facts, with key dates and people.
	Legal forum • What legal fora (courts, tribunals, committees, etc.) are available? • Which legal forum/fora are you likely to use?
	Law • What are the main legal arguments you will make? • What are the main counter-arguments you expect to see? How will you respond to them? • What are the arguments on admissibility, where relevant? • What further (legal) research needs to be done?

	Evidence • What is the evidence that you will rely on, such as witnesses, experts, data, and reports? • Who will be producing a Medico-Legal Report in the case? • What steps need to be taken to obtain additional evidence?
	Remedies • What are the financial and non-financial remedies that you will claim on behalf of the survivor? • Explain how your remedies align with the strategic objectives set in the case?
ADVOCACY AND CAMPAIGNING	**Advocacy Plan (where the case is public)** • What are your advocacy goals? • Who are your main advocacy targets? • Who are your advocacy messengers? • What are your advocacy messages?
	Communications Plan (where the case is public) • Who is your main communications audience? • What are your messages? • Who are your messengers? • What tools will you use: social media, video, digital communications, press conferences? • What are the key media events in the life of the case?
	Community (where the case is public) • What broader community are you indirectly representing by litigating the case? • How can you engage this community?
PRACTICALITIES	**Timeline and Milestones** • What are the major milestones in the case? • How long will the litigation take?
	Ensuring the Survivor's needs are met • What other types of support does the survivor need (medical, psychological, social, etc.)? • Can you refer the survivor to the appropriate services to cover those needs?

	Financial and Administrative • What types of costs will be involved in the case (travel, translations, court fees, lawyers' fees, investigators' fees, etc.)? • What is the total budget for the case?
	Risks • Is the case confidential? • What are the security risks (physical, documentary, electronic) and how can you mitigate them? • Are there costs risks?
NEXT STEPS	• What are your immediate next steps? • When will you complete them by?

ANNEX B
CASE SELECTION CHECKLIST

MANDATE & EXPERTISE	• Does the case fall into your own or your organisation's mandate and expertise?
SURVIVOR CONSIDERATIONS	• What is the survivor's objective in the case? Does the survivor seek acknowledgment, compensation, guarantees of non-repetition, or something else? • Are the objectives of the survivor compatible with your organisation's objectives? • What needs does the survivor have (e.g., medical, psychosocial, legal, and socioeconomic) and how do these relate to the legal issue? • Is pursuing the legal case likely to have an impact (either positive or negative) on these needs? • Are relevant professionals available to assist in considering the survivor's support needs? Can this support be maintained on an ongoing basis during the case? • Is the survivor currently receiving other support (consider medical, psychosocial, legal, and socioeconomic support)? What support are they not receiving? How do you fit in? • What are the likely impacts/risks of a negative case outcome on the survivor given their particular needs? • Are there protection concerns for the survivor or their family? If yes, can these concerns be managed?
CASE CONSIDERATIONS	• Where did the case come from? Was it referred to you by another organisation/partner? • Who else is working on the case? What would be your organisation's relationship with them? • What role would you play in the case (e.g., sole representative, co- representative, third party, or advisor)? • What information/evidence is available and how strong is it? If evidence is not sufficient or not strong, what is the likelihood and cost of obtaining additional evidence to support the case?

	• Are there protection concerns for you, your partners, or anyone else in the case? If yes, can these concerns be managed? • Where is the survivor based? If they are based in a different jurisdiction, can you work with a partner organisation that can support the survivor within their jurisdiction over the life of the case?
CASE STRATEGY	• What legal avenue(s) are available (e.g., domestic, regional, international)? • What are the advantages, disadvantages, or procedural obstacles of each legal avenue? • If you are considering an international or regional case, have domestic remedies already been pursued? Do you have clear information about the status/result of these proceedings and (if relevant) the date the final decision was made? • What is the likelihood and impact of a positive outcome and success for your survivor (in terms of their objective)? • What is the potential for implementation of a positive decision? You might consider the current situation in the country, the policy/attitudes of government, the implementation record of the country, enforcement possibilities, and the relative strength of the human rights mechanism involved. • What would success look like in the case beyond positive effects on the survivor? (e.g., positive change in jurisprudence or drawing attention to the issues of the wider community) • What is the potential impact of a negative outcome? • Are there concerns, considering the national and international context (including in the UNCAT, African Court, ECtHR, etc.), that pursuing the case could result in backlash, or a negative review of existing jurisprudence?
IMPACT	• Does the case pursue specific strategic objective(s)? • Does case reflect a specific practice/systemic problem and/or affect a specific group? • Does it address a 'systemic barrier to justice'?

	• What is the likelihood of the case setting a precedent or having an impact on (domestic) law/policy/public opinion? • Will the case progress legal standards/jurisprudence (either generally or within a specific mechanism) in favour of a specific group?
ORGANISATIONAL/ RESOURCE CONSIDERATIONS	• What are the envisaged resource implications for your organisation? (Time and cost) • Can you obtain specific funding for the case? Can the survivor contribute to costs? • Does your organisation have internal language capacity to work on the case? • How long will it take to complete the case at the national/regional/international levels? (Take into account research and drafting, liaising with partners, evidence preparation, survivor work and caregiving obligations, as well as the time it may take to receive a judgment) • Does the case link to other areas of your work? How? • Is there a potential conflict of interest with other survivors you represent? • Does the case overlap (even potentially) with any project/campaigning/advocacy issues in respect of which you have a clear policy position? If so, has the survivor been made aware of the policy position and does the survivor agree with this policy position? Is the survivor willing to instruct you on the case with the knowledge that you may be making public statements on these issues?

ANNEX C
INDIVIDUAL NEEDS ASSESSMENT FORM

Ensure that the survivor understands the purpose of an individual needs assessment and possible outcomes of the assessment and consents to the interview. Survivors should be given the opportunity to be accompanied by an individual of their choice, and also offered the possibility to request an interviewer of a certain gender.

Client name	
Date & location of review	
Name of staff member undertaking review	
Other individuals present	
Communication needs identified	Does the survivor require interpretation or translation? Does the survivor feel comfortable receiving information (e.g., about support organisations) in English?
Details of the torture and its impact	The views of the survivor should be at the centre of all decisions about support they may require. Attention should be paid to the survivor's assessment of the incident.

Support already being received (consider legal, social, economic, health (psychological/ physical), spiritual)	Agency/ Person Providing Support	Details of Support Provided	
Other support required	Agency/ Person who could provide support	Details of support needed	Can we provide a referral?
Likely impact of litigation on client	Is the survivor in a position to go through a (long-term) litigation process [e.g., can client give statements for a complaint; is client prepared to see specialists; can client give interviews to police; what are the vulnerabilities of the client to be aware of; what is the likely impact of the client's vulnerability on the client's ability to give clear instructions and on the strength of the case?]		
Required protection and support measures			

Recommended follow-up			
Has the survivor consented to having their information shared with other organisations as part of the referral process?			
Result of second assessment (include date)			
Recommended Follow-Up Actions	Follow-Up Actions	People Involved	Date Reviewed

ANNEX D
CLIENT CARE LETTER

[SURVIVOR ADDRESS/DATE]

Dear [SURVIVOR NAME],

Your case

Thank you for asking us to help you regarding [the DETENTION, TORTURE, or ILL-TREATMENT] you/your [RELATION] experienced in [COUNTRY/REGION].

I understand that you hope to [INSERT] and/or are concerned that [INSERT].

This letter

The purpose of this letter is to set out the basis under which we will carry out work on your behalf. This letter explains how we will manage your case and gives details of the person that will be responsible for the work on your case. Please do read the letter carefully, but do not hesitate to contact me if you have any queries or would like to discuss it further.

Responsibility for your case

I am a [LAWYER/CASEWORKER/LEGAL OFFICER, ETC.], and a qualified advocate in [SET OUT WHERE YOU ARE QUALIFIED AND WHO YOU ARE REGULATED BY]. I will look after your case on a day-to-day basis.

Contact

I can usually be contacted by telephone [TELEPHONE NUMBER] between 9.30am and 5.30pm on weekdays. You can also send me an e-mail at [EMAIL ADDRESS]. You can call [INSERT NAME] on [TELEPHONE NUMBER] if I am not available when you call me, and they will try to help with any queries.

Information about our organisation

[INSERT NAME] is an organisation working on [INSERT BRIEF DESCRIPTION]. If I am away from the office or unavailable (for example, because I am travelling or in a meeting) another member of staff will take a message and pass it on to me. If I am going to be away from the office for more than a few days, arrangements will be made for another member of staff to deal with any urgent matters which may arise.

We are happy for you to correspond by email, post, or telephone. [IF THE CLIENT HAS EXPRESSED CONCERN ABOUT EMAIL SAFETY, PLEASE ADD HOW THIS CAN BE ACCOMMODATED E.g., *If you would prefer to liaise with us via an encrypted form of email communication, we would seek to accommodate this by usin*g XXX].

Your instructions

We understand that you would like us to: [INVESTIGATE/WORK WITH X PARTNER TO/CHALLENGE…] and that your objective is [SET OUT OBJECTIVE AND NAME OF OTHER PARTY IF ANY]. *E.g., We understand that you would like us to investigate the options available to you in seeking redress for the treatment you suffered in [COUNTRY].*

You will:

- Send us [LIST RELEVANT DOCUMENTATION].
- keep us updated of developments and of any correspondence you receive in relation to your case.

We will:

- Develop next steps on the basis of the documentation you send us and advise you on the strengths and weaknesses of different options so that you know what is realistic, and so that you can make an informed decision about any next steps, taking into account what you – and your [RELATION if relevant] – are hoping to achieve.
- Put your interests first when representing you.
- Tell you about significant developments and update you regularly on progress as work proceeds.

Agreed next steps

[INSERT AGREED NEXT STEPS HERE – some possibilities are listed below]

Confidentiality

We will keep what you tell us confidential (unless otherwise agreed with you), unless we are required by regulatory authorities or by rules of law or professional conduct to disclose it. The confidentiality of email cannot be guaranteed.

Holding data, information, and documents

We consider that we have a legitimate interest to hold your data, information, and documents because this is necessary to establish, exercise or defend legal claims (whether in a judicial, administrative, or out-of-court procedure).

Files

After we have finished working on this case, we will write to you about the detailed arrangements for the storage and eventual deletion of your paper/electronic file.

Time scales

We will pursue your case as quickly as possible. However, the length of proceedings will largely depend on the body dealing with your case and the response(s) of the defendant(s). It may take a number of years to obtain a decision. The case may

finish more quickly if we achieve a settlement. We will keep you regularly updated of developments in your case.

Publicity

We will seek your permission before publishing any material relating to your case on our website or in public materials.

Complaints

We are committed to high-quality legal advice and client care. If you are unhappy about any aspect of the service you receive, please contact [INSERT NAME].

Depending on your jurisdiction, you may also include information about complaints to professional regulatory bodies.

Governing law and jurisdiction

This letter is governed by [INSERT COUNTRY] law and subject to the exclusive jurisdiction of the courts of [INSERT COUNTRY].

Understanding this letter

If there is any part of this letter that you do not understand, then please let me know. I would be happy to discuss it with you. We enclose two copies of this letter, which we have signed. Please sign below and return one signed copy of this letter to us by post.

Thank you for asking us to help you with your case.

Yours sincerely,

[SIGN BOTH COPIES OF LETTER HERE]

[Name]

Please sign here and return this letter to us to indicate that you have read and understood this letter, that you agree the terms of our engagement, and that you wish to proceed to engage [NAME OF ORGANISATION] in this matter on that basis:

Signature: ……

Printnamehere:…… Date:……

ANNEX E
AUTHORITY TO ACT FORM

I, **[SURVIVOR'S NAME]** authorise **[NAME OF ORGANISATION]** to act on my behalf in any judicial, administrative, or out-of-court procedures, including before regional and international human rights bodies.

I understand that any judicial, administrative, or other out-of-court procedures will deal directly with **[NAME OF ORGANISATION]** in relation to my case.

I understand that **[NAME OF ORGANISATION]** may provide information and documents about my case to others, in accordance with the terms of **[NAME OF ORGANISATION]**'s letter to me dated **[INSERT DATE OF CLIENT CARE LETTER].**

I authorise **[NAME OF ORGANISATION]** to:

- Receive information and documents from any judicial, administrative or other out-of-court procedures dealing with my case;
- Discuss my case with any judicial, administrative or other out-of-court procedures;
- Contact all persons and bodies necessary to progress my case, including in relation to any action taken to date or currently being pursued, any future action, and any medical or psychological practitioners in relation to my case and/or wellbeing;
- Provide information about my case to **[NAME OF ORGANISATION]**'s funders for the funders' own use in relation to any grant it has made or may make to **[NAME OF ORGANISATION]**;
- Refer to the assistance provided in my case on **[LITIGANT NAME/ ORGANISATION]**'s website and publications; and
- Instruct other appropriate persons to act on my behalf in relation to my case.

Signed: _____

Print Name: _____

Address: _____

Date: _____

ANNEX F
REVIEW OF DOCUMENTS FORM

Source of documents:

Date received:

Reviewed by:

Date of review:

Brief Description of Document	Date of Document	Summary of content of document	Location of document (include page number if in bundle of other documents)	Comments/ significance *(Mark key documents clearly)*

ANNEX G
CHECKLIST TO ASSIST WITH THE DECISION TO MAINTAIN OR CLOSE A CASE

MANDATE & EXPERTISE	• Does the ongoing work on the case still fall into your own or your organisation's mandate and expertise?
SURVIVOR CONSIDER-ATIONS	• What are the views of the survivor in relation to the implementation of their case? Does the survivor see any opportunities for implementation? • What are the objectives of the survivor in relation to implementation of the case? • In addition to the implementation issue, what other needs does the survivor have (e.g., medical, psychosocial, legal, and socioeconomic) and how can you take these needs into account? How do these broader needs relate to the possible termination of work on the implementation of the litigation decision? • Is stopping work on implementation likely to have an impact (either positive or negative) on the survivor given their specific needs? • Is the survivor currently receiving other support (consider medical, psychosocial, legal, and socioeconomic support)?
CASE CONSIDER-ATIONS	• How long have you represented the survivor and to what extent do they rely on your support? • When was the main litigation/judgment obtained? • Which (if any) aspects of the decision have been implemented? • Are there any foreseeable changes in the political context that could result in a more sympathetic approach to implementation from the State? • Is there a partner organisation and/or lawyer and/or government agency you can work with on further implementation? Have you worked with them in the past? How reliable and engaged are they? • Are there any partner organisations and/or lawyers whom you could talk to in order to try to obtain suggestions of other avenues to pursue? • Are there any other steps that could still be taken to advance the implementation of the case? What are they?

CASE STRATEGY	• What aspects of implementation remain outstanding? • Are there serious obstacles to obtaining implementation of aspects of the decision? • Do the outstanding implementation issues include specific strategic objective(s)? • What is the likelihood of success for the client?
IMPACT	• What is the potential impact of not managing to make further progress on the outstanding implementation issues?
ORGANI-SATIONAL/ RESOURCE CONSIDER-ATIONS	• What are the envisaged resource implications? • Does the case link to other areas of your work?

ANNEX H
CASE CLOSURE CHECKLIST

The case and all related administrative work have been fully completed.	**Y**	**N**	**n/a**
The client has been informed that all work has been completed.	**Y**	**N**	**n/a**
All original documents which can be returned to the client have been sent to the client.	**Y**	**N**	**n/a**
Duplicate documents and emails have been removed whenever possible.	**Y**	**N**	**n/a**
Correspondence is stored in date order.	**Y**	**N**	**n/a**
All outstanding payments have been made.	**Y**	**N**	**n/a**
Any compensation has been transferred to the client.	**Y**	**N**	**n/a**
Any undertakings have been discharged and the discharge recorded.	**Y**	**N**	**n/a**
All issues and / or complaints raised by the client have been resolved.	**Y**	**N**	**n/a**
A final risk review has been carried out and any identified further action has been undertaken.	**Y**	**N**	**n/a**
If necessary, contact has been made with our professional indemnity insurers.	**Y**	**N**	**n/a**
Any agreement made with the client to use/continue to use the case for publicity purposes is on the file.	**Y**	**N**	**n/a**
Steps taken to archive and record the date for destruction of documents (where appropriate).	**Y**	**N**	**n/a**
File closing letter sent to the client.	**Y**	**N**	**n/a**

REDRESS is an international human rights organisation that delivers justice and reparation for survivors of torture, challenges impunity for perpetrators, and advocates for legal and policy reforms to combat torture. Our cases respond to torture as an individual crime in domestic and international law, as a civil wrong with individual responsibility, and as a human rights violation with state responsibility.

redress.org

@REDRESSTrust
Company/REDRESS

REDRESS

Ending torture, seeking justice for survivors