DATA MANAGEMENT

SEXUAL EXPLOITATION AND ABUSE (SEA) RISK MITIGATION CHECKLIST

Applicable to Displacement Tracking Matrix (DTM); Information Management and; Monitoring and Evaluation (M&E)

IOM is committed to the protection against sexual exploitation and abuse (PSEA) in all its work. Sexual exploitation and abuse (SEA) occurs when an IOM worker or partner facilitating access or providing services and assistance use their position of power and trust to sexually abuse and/or exploit communities and beneficiaries. ***This Checklist supports IOM workers in preventing, mitigating and responding to SEA in all activities involving direct data collection with affected communities, individuals and beneficiaries, and data management. It is especially relevant for Displacement Tracking Matrix (DTM) programmes, but also for Monitoring & Evaluation (M&E), and Information Management (IM) components of wider IOM programmes.***

IOM seeks to prioritise safety and dignity in its programming, and to ensure meaningful access, accountability, participation and empowerment for all individuals it assists. Sexual exploitation and abuse (SEA) can occur in every type of programme where IOM workers and partners interact with affected communities, and assisted individuals, but each programme has its own set of distinct risks. There are important SEA risk considerations for activities involving data management, as they often require close interaction with communities, especially vulnerable individuals, creating opportunities for SEA. ***This Checklist supports IOM workers in preventing, mitigating and responding to SEA in data management interventions. It is especially relevant for Displacement Tracking Matrix (DTM) programmes, but also for Monitoring & Evaluation (M&E), and Information Management (IM) components of wider IOM programmes.*** It should be used in combination with the ***Proposal Development SEA Risk Mitigation Checklist,*** the ***Beneficiary Registration, Targeting & Selection SEA Risk Mitigation Checklist*** (as applicable), as well as ***the Chapter on Data for PSEA as part of IOM's Information Management Handbook (forthcoming) SEA Risk Mitigation Checklist for Partnerships (as applicable).***

For more information regarding existing sectoral SEA Risk Mitigation Checklists, contact IOM's global PSEAH unit at PSEAH-SH@iom.int.

If unchecked, **a range of SEA risks can emerge in activities involving data management.**

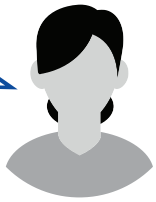
Examples of Sexual Exploitation and Abuse (SEA) situations in Data Management

1. Data collection tools and activities must never actively encourage the sharing of sensitive information, especially on issues related to SEA. Failure to adhere to this principle may result in serious risks and lead to harmful consequences[1].

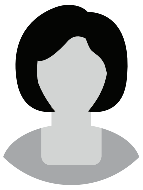
> *"During the focus group discussion, the facilitator asked if any IOM staff had ever solicited sex from us in exchange for assistance. I said that this had happened to me once and that I initially refused, but my family desperately needed the assistance. So, in the end, I gave my phone number to the IOM staff in exchange for assistance. My neighbour was in the focus group discussion and told what I said to others in the community. I fear that the abuser may learn that I spoke about the incident and retaliate. I also feel that my reputation is at risk."*

2. Enumerators may exploit their power over respondents, using it as leverage to commit SEA. This risk is heightened by the fact that enumerators can act as de facto "gatekeepers" of assistance, i.e., they control information that may lead or facilitate access to aid.

> *"An IOM enumerator told me that if I answered a survey, I would receive help. I don´t know how to write and read, and I told him that. He said that he could help me, but only if I let him touch me".*



3. Information provided by respondents may be used as leverage to commit SEA, either by those involved in the activity or external parties (in case of information breaches, for example).



> *"A quote from me criticizing the community leader, along with my name, was included in an IOM survey report. My neighbour, who is a volunteer with IOM, accessed the report and has demanded sexual favours in exchange for not disclosing this information to the community leader".*

[1] Support to minimize risks is available by contacting the PIM Field Support Network (PIM-Support@iom.int). Guidance is available at: https://dtm.iom.int/dtm-partners-toolkit/guide/dtm-prevention-sexual-exploitation-and-abuse

If not properly considered and addressed, SEA risks can surface at **different points in the data management cycle:**

a. Methodology and tool design

> *"An IOM enumerator asked me if I knew how to report bad behaviour from IOM workers. I said that IOM´s system is easy to use. In fact, I do not know how to report something like that, and I never reported it, I have only used the WhatsApp number to thank IOM for the NFI kit my family received last month. But the enumerator assumed that I had made a report about an IOM worker's bad behaviour. So, he told me that unless I accepted to go out with him on a date, he would tell IOM staff about my complaint, and they would block me from assistance".*

- Data collection activities must **never** include questions about sensitive information, such as SEA incidents, or deliberately solicit information that can reveal complaints of SEA, as this results in harmful consequences.
- Data collection tools must **never** include questions that only individuals who have used complaint and feedback mechanisms can answer. Complaints and feedback mechanisms are confidential, and this would enable complainants to be identified. It compromises their safety and access to further assistance.

b. Field data collection planning and preparation

> *"I was not informed that there would be a registration happening last week, so I was not home when the enumerators came. I contacted the IOM team to try to register the following day, but the staff I spoke with said that he would make an exception for me, but only if I accepted to meet him alone in a bar".*

> *"After responding to a household survey, I notified the IOM enumerator that one of his colleagues is asking for sex in exchange for food parcels. I then learned that the IOM enumerator told the abuser about what I said".*

- Data collection activities must be planned in advance and executed in a manner that ensures the convenience and safety of participants. This involves timely and clear communication about the purpose, location, date, and time of these activities. Individuals should also be informed that nothing can be asked in exchange for participation, registration and assistance.
- Field data collection teams must receive training on PSEA prior to deployment, including:
  - Never ask for anything in exchange for assistance and for facilitating access to assistance.
  - How to safely reports allegations of SEA, through the established channels and why.
  - How to share information about available support services with those who may need them
  - Confidentiality, i.e., **not** share SEA cases they become aware of with others.

c. Field data collection implementation

> *"The local NGO employee is asking for sex in order to register my name on the list for IOM assistance"*

> *"We fled our village without our men, and moved into this abandoned building, where nobody has helped us. Last month, IOM enumerators finally came to ask what we need. We answered all their questions, and then they said that they could inform people in the capital that we need help, but only if we show them how grateful we are. They told us that nobody knows that we are here, and nobody will come to help us if we are not "nice" to them."*

- Data collection activities must be planned and implemented in accordance with the risk mitigation measures outlined in sections 3 and 4 of the Checklist (below); these include actions such as, mandatory PSEA training for field data collection teams prior to deployment, monitoring of activities by supervisors to identify and address emerging SEA risks, etc.

d. Transferring storing and analyzing data

> *"Survey forms were misplaced and found by an IOM employee. He identified the woman who had answered the survey, and explained to her that he was in possession of sensitive information about her. He then told her that he would not share the information with others in the community, as long as she agreed to have sex with him".*

- Practical modalities should be considered and implemented to ensure safe recording, transfer and storage of data, these must address potential risks associated with information loss and breaches.
- All physical and electronic data files should be stored in accordance with a data safety management plan, including security measures to prevent information leaks.

e. Data dissemination and use

- Communities, groups and individuals sharing sensitive data must not be singled out and identifiable throughout the entire data management process, especially when sharing information with external audiences and making it publicly available.
- Details of SEA cases should not be shared with third parties - these should be reported through IOM´s reporting channels – We Are All In platform or OIOintake@iom.int.

> *"Women told DTM enumerators that the local NGO employee was asking for sex in exchange for including their name on the list for IOM assistance. This information was published online, alongside the name of the village. The police went to interrogate the women in the village and threatened them with jail-time if they did not disclose the name of the NGO employee. Local DTM staff were also threatened".*

RISK MITIGATION MEASURES FOR ACTIVITIES INVOLVING DATA MANAGEMENT

PROPOSAL DEVELOPMENT[2]

1. Allocate resources to PSEA under the activity´s budget.

> *For further guidance, please consult the* ***Proposal Development SEA Risk Mitigation Checklist.***

2. Follow IOM guidance on data for PSEA[3] when the proposal is drafted to ensure that the office only commits to feasible, safe, ethical and effective data management[4].
3. Allocate resources to support data protection under the activity´s budget, in line with the data management plan.

METHODOLOGY & TOOL DESIGN

1. Design the data activity by identifying the specific purpose for the exercise, as well as how information collected will be used. At this stage, contact Protection Information Management Field Support Network (PIM-Support@iom.int) for assistance, if needed.
2. When designing data collection tools and assigning data collection methods:
   - **Never** include questions about SEA incidents or deliberately solicit information that may result in disclosures of Gender-Based Violence (GBV), Child Protection (CP) or SEA cases. Questions **NOT** to be included: *"Do you know if anyone in the community has been asked for sex in exchange of assistance by an IOM staff or any other aid organization?".*
   - Questions are safe and appropriate to ask for the intended respondent group (e.g.: consider setting where data will be collected, who will be present when the information is shared by the respondent, etc.). [5]Examples of safe and appropriate questions include: *"Do organizations inform the community that all services/ assistance provided by humanitarian agencies are free and should not be exchanged for anything at all?"* or *"if there is misbehavior, or something concerning in the behavior of an aid organization staff, is there a system/mechanism/focal point that the community can use to complain?"*
   - **Never** include questions that only individuals who have used feedback and complaint mechanisms can answer. This would enable them to be identified and would breach confidentiality. It also compromises their safety and access to assistance.

[2] *For detailed guidance, see the corresponding* ***Proposal Development - SEA Risk Mitigation Checklist.***
[3] *https://dtm.iom.int/dtm-partners-toolkit/guide/dtm-prevention-sexual-exploitation-and-abuse*
[4] *Consult PIM_Support@iom.int for support on including only feasible, safe, ethical and effective data management content in the proposals.*
[5] *For guidance, see: DTM for Prevention of Sexual Exploitation and Abuse (PSEA) . The Do No Harm Checklist can help in making this determination.*

- Assigned data collection methods (e.g.: key informant interview, focus group discussion, household survey, etc.) enable obtaining the information sought[6], and are safe and appropriate for the intended respondent group.
- Only information that will be used is collected. A Data Analysis Plan (DAP) is prepared before finalizing the questionnaire -- the DAP includes a description of the analysis you plan to conduct for the result of each question and how each piece of information will be used[7].
- A Protection/GBV specialist is consulted to review and greenlight the data collection tool prior to its administration.

> ⚠ *Do not collect personal data that will not be used!*

3. Develop a plan for safely and securely managing data for all stages of the activity (collecting, transferring, storing, analyzing and destroying the data collected).
4. Whether using digital data collection, sharing, storage and analysis software, or paper-based solutions, take appropriate measures to protect the information in line with protocols outlined in the activity´s data management plan.

PROJECT SET-UP

1. Check with Human Resources (and IOM's PSEA Focal Point) that staff and related personnel[8] working in the activity have been vetted, received mandatory training on PSEA and signed a Code of Conduct[9].
2. Train all staff and related personnel working in the activity, especially field data collection teams, receive training on data protection[10], mainstreaming Protection in data and analysis activities, and safely managing incident disclosures[11].
3. When working with partners[12]:
   - All contracts and MOUs signed with implementing partners, (financial) service providers, traders, vendors, government counterparts etc. contain PSEA clauses whereby partners commit to mitigate and respond to SEA[10].
   - Assess all implementing partners involved in the project have been assessed for PSEA capacities through the United Nations Partner Portal, develop a capacity development plan jointly with the partner[13], and support them in meeting minimum standards on PSEA.
   - Implementing partners, service providers, traders, vendors, government counterparts are monitored to ensure adherence to PSEAH standards and commitments

> *For further guidance, please consult the **SEA Risk Mitigation Checklist for Working with Partners.***

For further assistance on assessing the PSEA capacity of your partners, contact IOM's PSEA Focal Point in your mission and/or IOM's global PSEAH Team (PSEA-SH@iom.int).

4. Strengthen or establish safe and accessible complaint and feedback mechanisms (CFMs), ensure procedures are in place for handling SEA complaints, including referring survivors to assistance and reporting SEA using IOM's reporting channels (*We Are All In* platform and OIOintake@iom.int).[14]
5. Raise community awareness of PSEA. Context- and culturally-appropriate awareness materials (such as posters and pamphlets), informed by community needs and preferences, on staff conduct and/or that aid is free and/or how to report misconduct are visible and/or handed out to beneficiaries/community members in the local language(s), in visual form, or communicated orally to beneficiaries/community members. This message is reinforced throughout the activity.

   For awareness raising materials on PSEA, contact IOM's PSEA Focal Point in your mission and/or IOM's global PSEAH Team (PSEA-SH@iom.int).

FIELD DATA COLLECTION, PLANNING AND PREPARATION

1. Train field data collection teams Protection concerns and how to safely respond to a complaint of SEA, including on sharing accurate information on services, how to contact the PSEA Focal Point[15], and how to report through IOM´s reporting channels: *We Are All In* platform or OIOintake@iom.int.
2. Provide field teams essential information to carry with them on:
   - Available complaints and feedback channels
   - Protection/GBV services available in the target area[16].
   - Contact details of the PSEA Focal Point(s).
3. Ensure focus group discussion sessions are homogenous – i.e.; all participants have the same gender, are from the same age group, hold similar positions in the community in terms of power; etc.

> ⚠ *Data collection activities focusing on sensitive issues, must be led and executed by PSEA, Protection and GBV experts, rather than DTM, M&E, IM or data experts.*

[6] *For further information, please refer to DTM Methods and Sources for Data Collection webpage. Tailored support is available through the Protection Information Management Field Support Network: PIM-Support@iom.int*

[7] *A DAP (Data Analysis Plan) template can be found on the DTM Analysis webpage.*

[8] *This includes all types of workforce, regardless of type and length of contract, for example, hourly workers, volunteers, etc.*

[9] *For more information on Human Resources aspects pertaining to PSEA, please refer to section A2 of the IOM's PSEA Toolkit & Checklist.*

[10] *For more information on IOM´s Data Protection Policy and compliance procedures, please refer to IOM Data Protection Manual and the Data Protection Checklist.*

[11] *For useful resources, see: https://dtm.iom.int/dtm-partners-toolkit/trainings. Contact the Protection Information Management Support Network (PIM-SUpport@iom.int) for assistance, if needed.*

[12] *For more information on assessing and supporting partners on PSEA, please refer to section B1 of the IOM's PSEA Toolkit & Checklist.*

[13] *For reference, see: Sample Template for Action Plan on PSEA.docx - Google Docs*

[14] *For more information on complaints and feedback mechanisms, please refer to section B3 (Complaints and Feedback Mechanism) of the IOM's PSEA Toolkit & Checklist.*

[15] *For further information, see: Trainings for DTM and Partners. For detailed information, please refer to key messages in Box B below.*

[16] *For example, enumerators/facilitator can use the GBV Pocket Guide.*

4. Unless the activity is conducted by Child Protection (CP) teams and actors, refrain from engaging minors (< 18 yo)[17].
5. Plan data collection activities, especially household surveys and focus groups discussions, during times and at locations that are safe, appropriate and convenient for participants, especially the most vulnerable groups/individuals.
6. Provide communities information about the activity well in advance, including:
   - Purpose
   - Time(s)
   - Location(s)
   - What information is being collected
   - How data will be used and shared.

⚠ *For any data collection, and especially when the activity includes registration, communities are also informed that nothing can be requested from them in exchange for having their names registered. For registration leading to assistance, communities are also informed that enumerators conducting the registration are not responsible for beneficiary selection and therefore cannot influence decisions or add names to lists.*

7. Field coordinators instruct enumerators on protocols to be followed to reduce SEA risks in household data collection:
   - Whenever possible, enumerator teams do NOT enter respondents´ homes.
   - If entering respondent´s homes, they ensure that the respondent is not alone; and that there is a female enumerator present if the respondent is a woman.

BOX A: CONSIDERATIONS ON GENDER-MIXED TEAMS

Programmes should take concrete steps to engage women as frontline workers, enumerators, or facilitators as part of SEA risk mitigation measures. However, meeting these requirements may be challenging in settings where context-specific cultural and security barriers exist. In such cases, consider the following options:

o Collaborate with other IOM teams (e.g.: Protection) within the operation that can volunteer women staff members to support these activities that involve close interaction with community members, especially vulnerable groups.

o Engage women-led local/community-based organizations, committees and groups to provide support and/or monitor such activities.

Consult the Protection/GBV/SEA specialist in your operation and contact the **Protection Information Management Field Support Network** (PIM-Support@iom.int) for guidance on safe and viable alternatives that can be explored in your context.

FIELD DATA COLLECTION IMPLEMENTATION

- Deploy Gender-mixed teams of enumerators and facilitators.
- Facilitators/enumerators interacting with women are female.
- In focus group discussions, note-takers are also women.
- Enumerators work in pairs (women and men).
- Enumerators/facilitators and other relevant field data collection staff wear badges and any other gear with logo at all times (except in contexts where this may create security risks to staff).

Please refer to Box A on considerations regarding gender-mixed teams.

For further guidance, please consult the ***SEA Risk Mitigation Checklist for Working with Partners.***

2. Direct individuals who wish to express grievances (e.g.: dissatisfaction with the data collection activity, etc.) to the available complaints and feedback mechanisms.
3. When conducting household-level data collection:
   - Whenever possible, enumerator teams do NOT enter respondents´ homes.
   - If entering respondent´s homes, they ensure that the respondent is not alone; and that there is a female enumerator present if the respondent is a woman.
4. In focus group discussions, participants are instructed to never share their names; if they do, these are not recorded.
5. In group discussions, inform participants that confidentiality can never be completely ensured in a group setting. Ask participants to discuss issues without providing details linked to specific individuals. If they do, these details are not recorded.
6. If the data collection activity is taped or recorded, informed consent (explaining who will access the information, why we are collecting the information and how and where the information will be available) is requested from respondents to record the audio.
7. If photos are taken during the activity, request informed consent from respondents and their faces are not visible (e.g.: photos are taken from afar, respondents are facing opposite the camera, etc.).
8. During spot checks of field data collection activities, coordinators verify the implementation of and adherence to these risk mitigation protocols by field data collection teams.

[17] Please contact DTM HQ for approval prior to any data collection activities involving direct engagement with children at DTMSupport@iom.int.

TRANSFERRING, STORING & ANALYSING DATA

1. An assessment of risks is conducted prior to data transfer, analysis and storing[18]. This will enable the identification of risks, such as that sensitive and/or personal identifying information is leaked, and potentially used as leverage to commit SEA.
2. Safely and securely transfer data (e.g.; digital, paper-based forms, photos, audios, transcripts) from the field to the office, following protocols outlined in activity´s data management plan to minimize the risk of information leak and breach by people inside or outside IOM who should not have access to the data. From the onset, define who should have access to which level of information; this will reduce the risk of information being unduly accessed or leaked, and potentially used as leverage to commit SEA.
3. Safely and securely store data, make it only accessible to those who need it (e.g.; hard copies are kept in locked cabinets, digital forms/information are password protected, and stored in safe databases etc.).
4. Anonymize personal identifying information (PII) before making it available for analysis[19].

⚠ *PII is only accessible to those who need to access it in support of programming decision-making and action.*

5. Promptly report incidents related to data breach and lost or stolen questionnaires to supervisors and managers.
6. Destroy project forms, hard copies and data-files, including any identifying or sensitive information, 180 days after programme closure.

DATA DISSEMINATION & USE

1. Assess risks prior to data dissemination[20]. This will enable the identification of risks, such as that sensitive and/or personal identifying information is disseminated, and potentially used as leverage to commit SEA
2. When sharing personal identifying information, ensure conformity with IOM´s Data Protection Principles and Manual, and that purpose is defined and acceptable; alternatives are explored before sharing individual data (e.g.: provided in aggregate form, etc.).
3. Carefully review the data before publishing and do not share details of SEA cases. These must be reported through IOM´s existing channels: *We Are All In platform* or OIOintake@iom.int.
4. Never include individual responses or any other information that could identify individuals and families in final reports/products.

⚠ *When quotes from respondents are inserted into documents, present these in a way that does not allow the individual to be identified. For example, not sharing information regarding the location of the respondent, the gender or any other individual attributes.*

BOX B: KEY STEPS IN RESPONDING TO A COMPLAINT OF SEXUAL EXPLOITATION AND ABUSE (SEA)

1. Ensure SEA survivor gets the assistance they need

- Address **urgent needs** immediately, including medical and safety.
- Find a **safe location** for you and the survivor to speak.
- Explain **mandatory reporting** to the survivor: if the survivor tells you that an IOM/ any aid worker committed SEA, you have an obligation to report to your organization; give the survivor the option of choosing if they want their personal information to be included in the confidential report to investigators or not.
- Inform the survivor about **available services** - know who your **service providers** are (Health, Safety, MHPSS) and use GBV/ CP/Protection **referral pathway**, if there is one.
- Ensure **informed consent** when referring to services: ensuring that a survivor agrees to access services on the basis of their having full information, including risks and benefits; them being competent to decide; and no coercion, threats or promises of benefits being used to secure that consent.
- Remind the survivor they can **seek services later**.

2. Report through existing mechanisms

- IOM's ***We Are All In*** Platform or OIOintake@iom.int
- In case you need further support, contact your PSEA Officer or Focal Point.

BOX C – USEFUL RESOURCES

- IOM's PSEA Toolkit and Checklist
- IOM Data Protection Manual
- IOM Data Protection Checklist
- DTM for Prevention of Sexual Exploitation and Abuse
- DTM and Partners Do No-Harm Checklist

[18] The Do No Harm Checklist can be used to support the assessment.
[19] Contact PIM-Support for help on how to do it.
[20] The Do No Harm Checklist can be used to support the assessment; for more information on data sensitivity, please consult the DTM Data Sharing Guidelines webpage.