LEARNING EVENT ON RISKS LINKED TO CVA

PUTTING BENEFICIARY PROTECTION AND DATA PROTECTION AT THE HEART OF OUR WORK

26 NOVEMBER 2019, DAKAR – SENEGAL

KEY MESSAGES

The humanitarian sector faces a real risk of a major data breach: there is no time to be complacent. Having a data protection policy at an HQ level is not enough. Responsible data management and data protection can feel overwhelming for CVA practitioners who have not been exposed to digital risks and data protection frameworks before. Although it will be a complex and difficult undertaking, we must try to do better. It's time to reprioritize this topic on our collective agenda.

RECOMMENDATIONS FOR ALL ACTORS

- Information is power. Empowering our beneficiaries to understand the implications of the data we collect about them and how it's managed is critical. That means real informed consent.
- Managing data responsibly means access to aid is not conditional upon the agreement to give biometric or personal data that can put beneficiaries at risk.
- Roles and responsibilities around managing protection risks and data protection should be clarified, and implementing teams at field level should be aware of the set up. We should not assume that stakeholders along the programme delivery chain or involved in the process know what they have to do (including sub-contractors, regulators, local agents and field staff).
- In countries where we operate, regulations and data protection national agencies sometimes already exist: it's everyone's responsibility to be aware of them and ensure compliance. They should also be used to inform policies and raise awareness on challenges and gaps in countries without such regulations in place.
- Setting gold standards in data protection is important to ensure progress and drive efforts in the right direction, but we need to break it down into small steps to build the confidence of all stakeholders – particularly field teams. We must prioritize getting the basics right.
- Collaboration is key to success – we must invest in increasing the interconnection and dialogue among all stakeholders. Capacity building is a two-way process, which should draw from all stakeholders' expertise. We must invest in building the necessary understanding of digital, humanitarian principles, protection and data protection to make decisions and ensure quality and accountability.
- While we know that learning by doing is often the way to progress in the humanitarian sector, innovative approaches must be challenged before they are tested on beneficiaries. Can the commitment to "do no digital harm" be ensured?

USAID
FROM THE AMERICAN PEOPLE

CaLP
The Cash Learning Partnership

RECOMMENDATIONS FOR IMPLEMENTING TEAMS

- All interventions impact social dynamics and generate different risks for different groups. Mitigation measures also generate new risks. It's important to keep the conversation going with beneficiaries who know better the types and level of risks our interventions can create and their capacities to face or mitigate them. They can help programme teams to address the key tensions identified during Douala event.
- Risk analysis must be integrated across teams and be context specific. There will not be a zero-risk option, but this will enable informed decision-making, programme design and adjustments along the way.
- There is a need to understand better the whole chain of stakeholders involved in financial transactions. For example, it is important to build an understanding of regulations and regulators' work.
- There is no perfect blueprint when it comes to protection and data protection – if a solution has worked in one place, it should not be assumed it will work just as well in another context; adjustments and ongoing sensitization is always needed.
- Don't take the 'us' and 'them' attitude in working with the private sector; the incentives may not be aligned, but taking a 'partnership' rather than 'service delivery' approach always pays off in the long term.

RECOMMENDATIONS FOR DECISION-MAKERS (DONORS, SENIOR MANAGEMENT STAFF IN IMPLEMENTING AGENCIES)

- Extensive control systems applied to CVA should be applied across humanitarian programming, regardless of the modality, as they have proven efficient to spot fraud and protection issues.
- Protection and data protection tools, such as the 'Safer Cash Toolkit' are useful, and efforts to make them user-friendly, accessible and easy to integrate to other existing resources are appreciated. But sharing tools is not enough, field practitioners need support to take up those tools and actually use them.
- Innovation and technology are important, but questions of accessibility and usage of the mechanisms (such as feedback mechanisms, delivery mechanisms) must be considered as a priority. These choices need to be driven by recipient preferences, and donors have a role to play in ensuring these considerations.
- Though it may not be possible to keep up with new innovations, it is important to maintain a dialogue with regulators to be aware of forthcoming developments.

RECOMMENDATIONS FOR PRIVATE SECTOR ACTORS

- Reaching out to Cash Working Groups (CWGs) and humanitarian agencies can increase your visibility and showcase your work in humanitarian fora. Humanitarian actors are struggling to identify partners with enough capacities in some areas, so strong alternative solutions are required.
- Share expertise on the financial ecosystem and work with humanitarian actors on pragmatic and realistic solutions, from programme design and throughout the implementation phase.
- Link up with CWG and humanitarian actors to understand humanitarian principles and specific vulnerability factors in humanitarian programming.
- Advocate for the development of data protection regulations and policies and work for their enforcement to protect the end-user and set the basics for a culture that promotes responsible data management.

RECOMMENDATIONS FOR GOVERNMENTS

- As governments are encouraged to develop technologies to scale up and accelerate the implementation of social programmes, this presents significant challenges linked to the management of personal records and the risks of misuse of those technologies due to lack of capacities and awareness of data protection. Biometric identification or financial digitalization are some examples.
- Strong communication and administrative systems (such as official email addresses for all government agencies, data protection policies and regulations, and training for civil servants) should be developed to support the digitalization of data as necessary.
- Ensure secure enough resources dedicated to support functions, technical assistance, consumer services and complaint mechanisms before new technologies are taken to scale.
- Official outreach services available within National Data Protection agencies should be promoted – for example if training and sensitization is part of the service, then this needs sufficient outreach to ensure uptake.