24th Feb 2021 Cash Hub Webinar Summary Points

Topic: CVA and Data Protection

Speaker	Summary Takeaways
Joseph Oliveros, Cash Innovations Senior Officer, IFRC	**Introduction to CVA and Data Protection** IFRC has recently published guidance on CVA and Data Protection based on consultation with near to 20 National Societies, two of whom we will hear from in this Webinar. In this introduction we would like to focus on 3 key questions: ▪ *Why talk about CVA & Data Protection?* ▪ Although data protection is not new, there has been heightened awareness on risks and impacts related to data protection in recent years because: - We are collecting more data particularly in CVA (assessments, beneficiary registration, monitoring/evaluation, audit), and a good portion of that relates to affected individuals, which could be private and sensitive. - Digitalization is accelerating our use of digital tools and technology: digital payments, mobile data collection, data management. Shift to digital means increasing risks to individuals in terms of their privacy, misuse, unauthorized access, unsecured sharing and storage, beneficiaries may not have control over their data. - Laws and regulations are changing. E.g. GDPR and other national laws. - Cash practitioners are asking for more practical guidance to analyze such risks and action them. Data Protection builds trust. No one wants to wait for a data protection breach that could impact the most vulnerable communities and the organization's ability to operate. ▪ Why was this guidance developed? ▪ There are existing materials out there (IFRC & ICRC policies, Handbook, CaLP, etc.), but they are perceived by some NS practitioners that they are quite high level, theoretical, not practical enough. We therefore needed to translate "legal" language to practical actions. ▪ The IFRC published recently a practical guidance on Cash Data Protection in consultation with legal data protection experts, NS's that have shared their experiences/concerns (close to 20 NS's and partners participated). Guidance is based on CVA processes and highlights how data protection principles could be systematically incorporated in these CVA processes. ▪ During our consultation with NS's we asked for sharing of issues and risks from those with programming experience, some observations have been made as follows:

	- Awareness of data protection is more on conceptual level. We needed to make the guidance as practical as possible. - Over reliance on Consent as a legal basis. For emergency context, we make a strong case to analyse potential legal bases and consider consent as a last resort, instead of the default. We have a section in the guidance showing a decision tree to help in this analysis. - Importance of data minimisation was agreed, but in practice this can vary and we will hear from two NS about this in this Webinar. - We asked NS's if their beneficiaries have raised concerns regarding their data. Answers depended on context, situation, and culture. People affected by sudden onset emergencies are likely to give as much info as you ask of them to gain assistance. That's why education is important. Both in terms of the rights to their data, and for NS to reinforce the responsibility to protecting data. ▪ So what now that we have the guidance? - You will need to contextualize the document for your context, programme, laws and policies. - We are working to get translation to Spanish, French and Arabic. - Developing training methodology for NS's to rollout training on Cash & Data Protection. - Let us know how we could support your NS's in awareness raising & advocacy. Use the Cash Hub remote help desk for questions and they will refer them appropriately. - We also ask you to be advocate for data protection in your organization and programmes.
Sophia Peponi, Cash Transfer Programming (CTP) Coordinator, Hellenic Red Cross (HRC)	**Hellenic Red Cross – CVA and Data Protection** ▪ Greece is subject to both EU GDPR and a new National Law supplementing GDPR (this defines for example, persons above 15 years old being able to consent to share data). ▪ Hellenic RC has appointed a private consultants' firm to undertake the Data Protection Officer function, and be responsible for data protection supporting HRC in his role as responsible for collecting, processing and storing data, and setting the means and the purpose for collecting data and processing it. ▪ On programmes where IFRC Greece/HRC are implementing partners to UNHCR for MPC to asylum seekers, then UNHCR is the data controller. ▪ HRC has been implementing Cash and Voucher Assistance (CVA) since 2016, and we are now implementing it across all sectors. We have recently undertaken programmes in relation to COVID-19, and there are plans for conditional cash for health, and plans for cash for protection. ▪ Based on previous cash interventions, either in emergencies or through our regular programmes, we have the capacity to quickly deliver cash assistance for 800 to 1000 household, with the current

	system and human resources in place, but looking to scale up further. ▪ HRC taking steps to fully comply with the data protection regulations. Cash Transfer Programming team has fully engaged with this initiative. This has included (amongst other activities): - A mapping of risks & gaps - considering data security - Forms for staff and volunteers to understand their roles in data protection - New information and consent forms for those we are asking to share data. ▪ There are a range of processes in delivering CVA that require consideration of Data Protection such as: Do we use a generic or personal email address for the KoBo account, who should be able to access the server that holds the data, who can access the master file, can we setup a server with different access rights, to minimise duplication risk we want to collect IDs for all in the HH over 15 but then this increases the amount of data we hold. ▪ Do we collect more data than we need, we must not just collect data out-of-habit it must have a purpose? ▪ Considering data sharing agreements. IFRC Greece/HRC has been collecting data as part of a programme as an implementing partner of UNHCR. We were able to negotiate what data we collected and what we shared. ▪ How the EU General Data Protection Regulation (GDPR) has impacted our cash interventions and time of response in emergencies. In Dec 2017 we were able to use data shared from local authorities which allowed cash transfers within 7 days. In July 2018, with the GDPR being implemented, it was not possible for the affected local authorities to share data (affected population lists) with HRC. The regulation was new, there was no data sharing agreement in place between HRC and the affected local authorities, the beneficiaries of their lists had not a prior information and consent for their data to be shared with HRC. Therefore, HRC decided to organise its own registration to collect affected population's data, which affected the timely response of the delivery of cash assistance. It took together with the registration process 4 weeks. In future we must work in preparedness to have data sharing agreements with prone to disasters local authorities/civil protection. ▪ We must understand who is the Data Controller of personal data. For instance, if there is a request from government to share data, this could be passed to the Data Controller for appropriate management. Especially important where a NS is an implementing partner. ▪ HRC's way forward on data protection is currently developing and includes drafting processes that are fully compliant, revising registration forms and consent forms. We are contextualising the IFRC Practical Guidance for Data Protection in CVA to the national law.

	▪ NS should make use of existing resources in National Society such as legal department, and always CVA staff should ask for assistance on data protection when we don't know. We should also share data protection good practice with sectors and other teams.
Dauda Mohammed, CTP and Livelihood Focal Point, Nigerian Red Cross	**Nigerian Red Cross – CVA and Data Protection** ▪ Nigeria has 140 million people and more than 250 ethnic groups. Nigeria has a range of ongoing and frequent crisis including conflict and natural disasters. ▪ Nigeria Red Cross (NRCS) has been using the data protection policies of IFRC and Participating National Societies (PNS) previously, but in 2019 the Nigeria Data Protection Regulations (NDPR) was issued. ▪ From 2015 NRCS has been working with ICRC using Cash Transfer Programming (CTP), and since 2018 with IFRC. In COVID-19 we have been responding with cash to support 8400 households with Cash and Voucher Assistance (CVA). ▪ Data protection is integral to our "Do No Harm" commitment, and we have taken a risk management approach. ▪ Leak of any data is unacceptable, and can cause targeting of recipients for violence or harassment. Even being associated with assistance from international organisations can lead to problems. ▪ Thinking about why people fear sharing data - In Nigeria the context is that the distribution of assistance is based around the population size, so people fear giving data if they fear there are few in their community because of a fear in the reduction in wealth distribution. - There are personal fears because they don't want to tell others if they are vulnerable. - They worry that if they give data they are being seen as recipients of assistance in the future and they may be attacked or there may be theft - There is a social stigma of being assisted - They fear that the organisation taking their data or processing their data will use it for their own purposes and negatively impact them. So sharing data is very sensitive. ▪ We need to think through each step in our data collection, storage, processing. Who collects the data, what we do with it, how do we store it, where does it go. ▪ Thinking about the principles of data protection practically: - Inform all actors (gov, management, staff, volunteers, communities, beneficiaries) of the requirements related to data protection. - Transparency of purpose - ensure all are aware of purpose of data collection and how it will be processed. - We minimise the data collected, and we minimise the data we transfer to FSPs. - Data is transferred securely and stored encrypted - A barcode system is used so that the NS relevant staff can trace who the data refers to but others can not.

	▪ In the COVID-19 operation in relation to informing communities and asking for consent in related to data collection and processing, CEA was crucial. ▪ A barcode system has been very helpful to allow us to anonymise data when sharing it. So only select staff can trace back the names of the data to the appropriate recipients. ▪ 3 practical recommendations: - Communication with all stakeholders especially the communities related to why we need the data and how their data will be collected, processed and safely stored is crucial. - Scanning through the data processing sequence at all levels to consider the data risk and how best to manage these risks. - Informing beneficiaries, we inform verbally and may include information on data protection in leaflets for beneficiaries.
Ben Hayes, Data Protection Legal Adviser, ICRC	**ICRC Key Takeaways and Key Actions** ▪ One key aspect we want to highlight relates to Community Engagement and transparency related to Data Protection and this is something we have worked on and are working on in ICRC. How do we communicate the data processing and the risks associated with data processing to the vulnerable communities we support. This is about transparency, and not specific to cash. ▪ Also worth considering choice, have people been presented with different options should they raise concerns about our use of intermediaries (e.g. Financial Service Providers) for example. ▪ Many in the humanitarian sector keep informed consent at the core of what we do, and this relates to transparency and building trust. However, in a data protection law context, informed consent has a specific legal meaning, and if the person (the Data Subject) consenting has no choice but to give consent to receive assistance, then informed consent is not going to be an appropriate legal basis for personal data processing since it may not meet the standard of freely given. The ICRC Handbook on Data Protection Chapter 3 provides significant information on this issue. That said, even if you are not processing personal data using the legal basis of Consent (but rather under another basis), it is still important that affected individuals have the opportunity to ask questions and are not compelled to participate in data processes where they object. ▪ Risk Management – the EU GDPR referred to by ICRC and many NS, as it is held up as the Gold Standard of Data Protection law, requires Data Protection Impact Assessments to be undertaken when the risk is above a certain threshold. The complexity of Cash data processing and the vulnerability of the communities we assist means that cash programmes will often meet this threshold. What we have found in practice, is that field staff may struggle to understand and deal with some of the underlying generic risks that are often there. Such as surveillance, or the risk that some entities in the data processing chain may misuse/repurpose the data. We

	sometimes call these structural data protections risks. Given that our beneficiary groups are not homogenous and that these different groups face different data protection threats and risks, how can we quantify how likely these risks are to materialise? A practical example, if you are dealing with an unbanked population that is not registered in the financial system then because of the proximity often of the financial system and the authorities there is greater risks for those unbanked than those already within the financial system. ▪ Data minimisation – great to see in the NS examples only sharing the essential data using pseudonymisation to mask identities, e.g. the barcode use in Nigeria. Limiting internal staff access to the data is important through internal controls is just also important. ▪ Mobile data collection – not limited to cash – most of the commonly used data collection system are cloud based and this can increase the risks, and we at ICRC have spent a lot of time looking at this. For some dataflows we have brought specific tools inhouse to mitigate the risks of loss of jurisdictional control of data, so Red Rose and Device Magic specifically. ▪ The relationship between different agencies and the responsibilities of different parties is important. So, for example, Hellenic RC referred to UNHCR which may have used their standard biometric data management system which partners can than use, however, the data protection risks then get more complicated. ▪ GDPR EU regulations requires the Data Controller to do some sort of adequacy determination before they pass data onwards, to for example, international organisations such as the ICRC or UN. What this adequacy determination looks like is unclear, but there could be additional risks if data sharing is not adequately managed. NS who may be acting as implementing partners will need to ask difficult questions of international organisations in relation to data protection, which it is appreciated can be challenging. ▪ When we are asked to share data with donors, we are asking ourselves what data, why do they need it, have we done a data minimisation review, can the data be anonymised or pseudonymised. ▪ Understanding who is a Data Controller and a Data Processer is also important, for those who are Data Processers they should just use the data for processing under the specific instructions of the Data Controller. If they are controllers it is much more likely they may try to use the data for other purposes. The challenge that this raises is that when we are offering anything other than pre-paid cards or sub-accounts, the financial service provider (FSP) is likely to be a Data Controller. Then challenging from a risk management perspective and contractual terms needs to be reviewed. ▪ Please do refer to The ICRC Handbook on Data Protection since this covers many of the things that we have spoken about.

Prepared by David Dalgado, Cash Hub team based on what was shared in the Webinar.