Questions and Answers - Responses to posted questions raised in the Data Protection themed Cash Hub Webinar held on the 24th February 2021 and those posted in the registration prior to the event.

Questions list:

Hellenic Red Cross

1) With respect to Data Protection how does HRC inform and train staff and volunteers.
2) How is beneficiary data consent undertaken in practice - is this explained to each individual and in their language, so they understand the implications of giving their consent? Or just mentioned in a community meeting?
3) When you are provided with data from local authorities on potential recipients what do you then do?
4) Could you share an example of a consent form with us?
5) Do you consider the use of the Red Rose system? And if you have used it before and now stopped can you explain why?
6) What was your strategy regrading data protection advocacy with government if they asked you to share your data?
7) How do you manage the sharing of data with donors (audit, reporting) and within Red Cross Red Crescent Movement?

Nigerian Red Cross

8) How is beneficiary data consent undertaken in practice - is this explained to each individual and in their language, so they understand the implications of giving their consent? Or just mentioned in a community meeting?
9) Could you share an example of a consent form with us?
10) Do you consider the use of the Red Rose system? And if you have used it before and now stopped can you explain why?
11) In the past we have shared beneficiaries names with FSPs for the production of cards prior to any cash distribution. How does data protection come in here?

General

12) Where can we find IFRC standard template of a data sharing agreement?
13) Is there any existing guideline for data disposal at the end of project life with partners?
14) With respect to when we do and do not need to get beneficiary consent please can you clarify?
15) Anymore insights on different data protection thresholds for one off CVA versus repeat payments?
16) How do you manage the data protection related to taking of images?

17) I have concerns related with 'free' mobile data collection such as KoBo.Is it safe enough to collect data (including sensitive information) using that platform?
18) Does the RCRC Movement share Beneficiaries' Data amongst itself?
19) With respect to RedRose use in Cash Transfer programming, I have heard of many National Societies stop using it when ICRC and IFRC are not paying for it and revert back to KoBo, in general is this the case.
20) Using a robust data management platform can be helpful to minimise risks/challenges etc. (e.g. SCOPE WfP) What is RCRC experience in this context?
21) What about the suggestions for reach those people who have not digital access?

Q	**Question (ed. for clarity)**	**Response**
	Hellenic Red Cross	**Sophia Peponi**, Cash Transfer Programming (CTP) Coordinator, **Hellenic Red Cross**
1	With respect to Data Protection how does HRC inform and train staff and volunteers.	There is no particular training currently. The HRC staff are expected to take part in a training on Data Protection as soon as the HRC policy is ready. At the moment all HRC staff have signed a form on data protection as an annex to their contracts (both core staff and short-term staff). HRC also has a form (an affirmation) that volunteers must read and sign, which is related to data protection and is necessary for their involvement in cash activities, especially registration and data collection. Before a cash intervention takes place the team (staff and volunteers) normally take part in a cash orientation session, which has a focus on the project and the implementation processes. Beneficiaries' information and consent is part of it as part of the registration process. As we move with the preparation of the Data Protection Policy in the National Society and the drafting of relevant forms or securing systems, we are making additions to the material of this cash orientation session so that a Data Protection component is part of it. So far, after the orientation session, a very good briefing to the field teams on mobile data collection was given, explaining why we collect this data, the importance of protecting the data (not sharing), and the procedures related to how we store the collected data.

2	How is beneficiary data consent undertaken in practice - is this explained to each individual and in their language, so they understand the implications of giving their consent? Or just mentioned in a community meeting?	Migration context: Before the enrolment of the beneficiary starts, the text of the consent is shown to the beneficiary to read in a physical piece of paper and in a language that the person can read. In case the person cannot read, a cultural mediator explains the content of the consent. The consent of the person is then orally collected by the CTP Officer who asks for it in order to click "yes" to the ProGresV4 database and start the enrolment process (start inserting information to the UNHCR database). During the Covid19 pandemic the consent content is orally explained before the enrolment starts. Domestic population: There are 3 different ways HRC collects the beneficiary's consent in the domestic cash interventions, depending on the set up of the project: a. Registration with physical presence: the applicant reads and signs the information and consent form in two copies. One is kept at the office the other is for the beneficiary to keep as it contains all their rights. *[standard practice]* b. Remote registration: the applicant prints the information and consent form, signs and then submits it as a scanned document along with the application form and the necessary supporting documents to the designated email of the project. The documents are checked and an appointment is fixed for the remote registration over a phone or video call using tablets. The form again starts with a "yes/no" choice for consent *[about to start implementing].* Online self-registration: The applicant reads the information and consent form on the online registration form and gives consent by clicking "yes" before he/she starts the online self-registration process. At the end there is a possibility to print the registration form *[about to start implementing].*
3	When you are provided with data from local authorities on potential recipients what do you then do?	An example from an emergency in 2017 (before the EU GDPR), we were able to receive the list by the affected municipality who had undertaken an assessment to register all the affected households with their technical teams. There were 3 levels of damages. We selected to work with the most damaged houses and the most vulnerable. In practice we split the affected area in geographical sectors and sent the registration teams to do home visits to targeted areas and households, pre-identified from the technical teams of the local authorities as the heaviest damaged. Having a list of standard vulnerability criteria (lonely elderly, disabilities, chronic diseases, heavy health conditions) we visited the heaviest affected households and we conducted short interviews to select and verify our beneficiaries on the spot. (Collecting minimum data via photos, such as IDs, bank accounts and respective supporting documents in case of disabilities, etc.). Household addresses, level of damage, #of household members was a very useful information that allowed HRC to gain time and

		have a very targeted response. This practice is not anymore compliant with GDPR in Greece unless there is a pre-agreement for data sharing and a prior beneficiaries' consent for this data sharing.
4	Could you share an example of a consent form with us?	This is currently being revised by HRC and is not ready for sharing at this time.
5	Do you consider the use of the Red Rose system? And if you have used it before and now stopped can you explain why?	We haven't used the Red Rose system in the Hellenic Red Cross. However, it had been presented to us as an "one solution tool" debit card/data management and analysis during the period 2015-2016 when different cash actors in Greece were exploring systems that would enable them to roll-out their cash programmes in the migration context.
6	What was your strategy regrading data protection advocacy with government if they asked you to share your data?	As far as it concerns the migration context, in case of data sharing requests, based on the data sharing agreement between IFRC and UNHCR, those need to be redirected to UNHCR, which is the data controller. IFRC has clarified the kind of information that can collect for this programme, which is reflected to the data sharing agreement with UNHCR. Therefore, there is no direct connection of the IFRC/HRC or advocacy on data protection with the Government. In domestic HRC cash interventions we haven't received so far, any request. However, in case that happens it will be based on a pre-agreement framework that will define first the minimum of information we can share and will allow prior information and consent of the beneficiary for data sharing with the Authorities. (i.e. cash in emergency response, pre-agreements with local authorities in prone to disasters areas). HRC Cash team and HRC as data controller does not share beneficiaries' data without an explicit consent of the beneficiary.
7	How do you manage the sharing of data with donors (audit, reporting) and within Red Cross Red Crescent Movement?	As explained in the presentation, as with the example of acting as an implementing partner to the UNHCR we can negotiate with the donor/partner what data we can and cannot share as part of being compliant with GDPR and the national regulations. HRC as a data controller cannot share beneficiaries' data, unless there is a prior consent of the beneficiary. The donor's requirement for audit or reporting reasons should be made known before the agreement and the registration process of the cash intervention. Each donor's/third party's request should be examined at

		an ad-hoc basis particularly for the outside of the Movement donors or private sector. So far, the HRC has not shared data with outside the Movement donors. As part of the process and for the RC/RC Movement donors in particular, this is under consultation, but in general will follow the steps described here. As soon as the request is known, the HRC will address to the DPO for consultation and come back to the donor with the minimum of the data we can share. We will then request form the DPO to adjust the informed consent form so that the donor is included and the beneficiaries have prior information and consent. HRC is currently revising the informed consent form so that we include IFRC as the donor of our current cash intervention under the National Response Plan for Covid-19, which is about to start. But this process is still ongoing. We expect that the revision will allow minimum data to be shared for auditing/reporting reasons. We also explore, by HRC own initiative, if spot checks of a small % of beneficiaries' files are allowed to take place. Perhaps a good practice would be for the National Society to prepare a short data sharing agreement to define this minimum data sharing and the percentage of spot checks. However, this is still under discussion.
	Nigerian Red Cross	**Dauda Mohammed,** CTP and Livelihood Focal Point, Nigerian Red Cross
8	How is beneficiary data consent undertaken in practice - is this explained to each individual and in their language, so they understand the implications of giving their consent? Or just mentioned in a community meeting?	Yes we have over 250 languages in Nigeria, so we have to ensure we are informing beneficiaries and seek consent in different languages. We do this at the community leaders level, youth and women leaders, section heads (such as religious heads) and at the potential recipients level. Nigerian Red Cross also established community resilience committees in any community we work in, if they do not already exist. These are trusted community members, and these community resilience committee members also help with the communication (although they also help with inclusion and exclusion error).
9	Could you share an example of a consent form with us?	The informing the recipient of the purposes of collecting data, how it will be processed and stored and transferred etc. and consent is on KoBo, and is asked verbally. For some, we may move to a paper soon since we are also wanting to generate success stories etc.

10	Do you consider the use of the Red Rose system? And if you have used it before and now stopped can you explain why?	Nigerian RC has an orientation of Red Rose and understand its potential. But we use KoBo, Excel, Magpi, and our own servers and phones in general.
11	In the past we have shared beneficiaries' names with FSPs for the production of cards prior to any cash distribution. How does data protection come in here?	On some programmes, Nigerian Red Cross may also share names with some FSPs, and to do this we inform beneficiaries of our intention and processes before we collect data and gain their consent. However, we only share minimal data on the beneficiaries, just to allow the banks to print what is needed. No data on phone numbers, locations, or vulnerability is shared.
	General Questions	
12	Where can we find IFRC standard template of a data sharing agreement?	**Joseph Oliveros**, Cash Innovations Senior Officer, IFRC & **James De France**, Senior Legal Counsel and Data Protection Officer, IFRC The Data Sharing Template is still in draft form, but a consultant will soon be brought on to complete the finalisation of this. It will then be shared with National Societies. For those with access to FedNet, some resources are currently available here: Policies, Guidance and other resources - IFRC - FedNet
13	Is there any existing guideline for data disposal at the end of project life with partners?	**Ben Hayes,** Data Protection Legal Adviser, ICRC In principle, data should only be retained for as long as it is needed to fulfil the purposes for which it was collected. At this point it should be delated. If certain data needs to be retained for auditing or archiving purposes it should be subject to a minimisation review to ensure that only the data needed for these purposes is retained. Archived data should be stored securely and no longer actively processed by the programme that collected it. Retention and deletion periods should be set at the start of the project and agreed with partners and service providers as far as possible. Where these entities act as processors, they can and should be instructed to delete the data and confirm/verify its deletion. If the partners are independent data controllers they may set their own retention periods.

14	With respect to when we do and do not need to get beneficiary consent please can you clarify?	**Joseph Oliveros**, Cash Innovations Senior Officer, IFRC & **James De France**, Senior Legal Counsel and Data Protection Officer, IFRC See page IFRC Data Protection and CVA guidance Page 21 -22 includes a decision tree.
15	Anymore insights on different data protection thresholds for one off CVA versus repeat payments - given Joseph's information about how people with new needs (e.g. immediately post disaster) seem to be more tolerant to providing info as a way of getting support?	**Joseph Oliveros**, Cash Innovations Senior Officer, IFRC & **James De France**, Senior Legal Counsel and Data Protection Officer, IFRC The same data protection considerations are to be applied regardless if the programme has a one off or repeat payments design. However, to the extent that the interventions will be ongoing, it may mean continued relationships/data sharing with partners (such as FSPs), or increased data collection requirements (such as monitoring surveys). Also, with respect to those with "new needs" being more willing to provide information, this provides a good example of why consent as a legal basis is probably not appropriate. For a repeat intervention, where participants are familiar with the process and there is some level of trust, it is more likely that consent as a legal basis for data processing may be possible (if a new or additional legal basis is needed, and recalling using consent as a basis has many challenges). Repeat payments, monitoring and engagement may mean continued efforts are required to ensure beneficiaries know where and how to raise data protection concerns or answer questions regarding their data, which should be integrated in the CEA plans.
16	How do you manage the data protection related to taking of images?	**Joseph Oliveros**, Cash Innovations Senior Officer, IFRC & **James De France**, Senior Legal Counsel and Data Protection Officer, IFRC IFRC has strict guidelines about when it is appropriate to take video and images and when consent should be used in those cases. In the future, it would be good to explore moving the information, consent and image/video to one digital platform like some other international organizations have done with a mobile application.
17	I have concerns related with 'free' mobile data collection such as KoBo.	**Ben Hayes,** Data Protection Legal Adviser, ICRC As explained in the Webinar most of the commonly used data collection systems are cloud based and this can increase the risks of unauthorised access to or non-humanitarian use of data. It can be difficult to

	Is it safe enough to collect data (including sensitive information) using that platform?	address these risks due to the cost and lack of alternatives. National Societies or partners may have access to mobile data collection apps of configurations that ensure data is hosted locally/within the country it was collected **Joseph Oliveros**, Cash Innovations Senior Officer, IFRC Kobo/odk is widely used in data collection for humanitarian action. There are however different instances or installation available, and verifying the security measures applied on those instances would be key, as well as the requirement of the programme or local regulations (e.g., data should remain in country). the IFRC is offering access to its kobo server (https://kobonew.ifrc.org), which has been reviewed with the IFRC IT department for data security, and NS's can request to use it if a cloud based solution is appropriate for them. **Info from IFRC IM:** There are three points of vulnerability for KoBo data: (a) on the handset, (b) in transmission, and (c) on the server. These are mitigated as follows: 1. on the handset, the data is normally available in clear-text on the handset until it is transmitted, so we recommend that the handset itself is encrypted (a standard Android feature) so that unless it is unlocked by an authorised user, the data cannot be obtained. Once transmitted, the data is normally deleted from the handset. 2. In transmission, KoBo uses TLS by default. 3. On the server, the data is as secure as the server, which depends on who runs the server. Some agencies, including IFRC, have chosen to set up their own server partly in order to guarantee the security of their data to a higher level than that provided by the freely-accessible servers. As an advanced feature, KoBo also supports end-to-end encryption of data payloads so that the data packages are encrypted with a public key at the moment that the form submission is finalised on a handset, and can only be decrypted by a matching private key held on an individual's local computer. This data is fully encrypted on the handset, in transmission and on the server, and needs to be downloaded from the server to a local environment prior to its local decryption. This of course renders inaccessible any of the server-provided reporting and analysis options.

		In practice, we've found that these points have always been sufficient to alleviate any data protection concerns on a technical level. Also, the real data protection vulnerabilities are rarely technical but far more often due to poor form design. So we also recommend that anyone deploying any form (whether using KoBo or any other tool) consider carefully whether there is any real need to collect personally identifiable information in the first place. Unless they are explicitly doing beneficiary tracking (in which case the most critical point of vulnerability is the server database where the full information about beneficiaries is brought together, which is not KoBo), there is rarely a need to do so. Data flows • Data is processed in AWS Data Center in Europe under the responsibility of IFRC. Kobo Inc. has a contract with IFRC to support and maintain the service. • There is no data sub-processing as per the existing clause in the signed contract. **James De France**, Senior Legal Counsel and Data Protection Officer, IFRC Please consider what data is strictly necessary before collection (whether on Kobo or not). It is likely to be the case that sensitive data is NOT needed.
18	Does the RCRC Movement share Beneficiaries' Data amongst itself?	**Joseph Oliveros**, Cash Innovations Senior Officer, IFRC & **James De France**, Senior Legal Counsel and Data Protection Officer, IFRC Not without a formal agreement, or in the event that there is an emergency necessitating immediate data sharing (in which case a formal agreement would be pursued in parallel) and with a sound legal basis.
19	With respect to RedRose use in Cash Transfer programming, I have heard of many National Societies stop using it when ICRC and IFRC are not paying for it and revert back to KoBo, in general is this the case.	**Joseph Oliveros**, Cash Innovations Senior Officer, IFRC It is important to differentiate the functions provided by Kobo (data collection) and RedRose (data management). For those looking for only data collection, Kobo is sufficient. If you'd like to manage data (I.e., link data sets from multiple surveys, manage beneficiary profiles, develop a payment list, integrate with FSP's-- which is both auditable and secured--you will need a robust database or a data management platform such a RedRose).

		Also, there is an integration between RedRose and ODK/Kobo, so these are complementary tools not one in lieu of the other. We have NS's that collect data via Kobo and upload data into RedRose for general data management. The benefit of using the ODK/Kobo that's directly integrated with RedRose is that data is synchronized directly on the RedRose platform, so you do not have to manage two systems. Also, the data collection interface is exactly the same. So if your staff and volunteers have been trained on Kobo Collect or ODK Collect already, there is no need to retrain them. In terms of NS's that have piloted the use of RedRose, we have good examples from Kenya Red Cross continuing to use the platform for non-IFRC supported projects and large scale programmes. The same with Pakistan Red Crescent that's been using RedRose for EA's and DREF's (cash and in-kind) and bilateral programmes (in-kind). There are considerations other than cost to ensure sustainable use of such a platform. See the analysis and recommendations from the RedRose Data Management Learning Review in the cash hub. There are also other lessons learned published in the RedRose toolkit in the cash hub.
20	Using a robust data management platform can be helpful to minimise risks/challenges etc. (e.g. SCOPE WfP) What is RCRC experience in this context?	**Joseph Oliveros**, Cash Innovations Senior Officer, IFRC The CVA Data Protection Guidance document pages 39-40 talks about data storage and data security. It is recommended to use robust data management solutions because they typically have built in functions to ensure encryption of data, access control, audit logs, backup, which are all important in safeguarding data. It is particularly important when data you collect grows/scales with your programme. The RedRose Data Management Learning Review in the cash hub also provides details on how robust platforms are not just useful to ensure timely and quality programmes but also essential in addressing risks related to data protection and accountability.
21	What about the suggestions for reach those people who have not digital access? Thank you	**David Dalgado,** Cash Hub, British Red Cross There are various examples for reaching people who do not have access to technology (such as mobile phones/network coverage). This can involve national society volunteers and staff travelling to interview these people taking their own devices to record the information. Transfer mechanisms also need to be considered carefully and adequately cater for these people, this could involve specific transfer mechanism for this group. How monitoring and follow-up will be undertaken also needs to be considered at the programme design stage.