CASH & VOUCHER ASSISTANCE

ICRC

BRIEFING NOTE FINANCIAL SERVICE PROVIDER DATA FLOW

(June 2024)

CONTEXT AND SCOPE

Cash-based assistance is one of the most significant reforms in recent years. There is no longer serious dispute about whether Cash & Voucher Assistance (CVA)[1] can significantly improve humanitarian aid as it puts power in the hands of affected people, increases choice and dignity, while also supporting local economies. ICRC has used cash transfers to support affected communities for decades, but as we grow the use of cash, *how* we transfer money to affected people have changed. Whist we can still hand over cash in an envelope, and often do, most transfers now are made using Financial Service Providers (FSPs). This includes bank transfers, remittance companies, prepaid cards, and mobile money. Using FSPs can be faster, cheaper, and delivered at a larger scale; they can increase transparency; they are discreet and as such can be more secure for the recipients and our staff; and they support financial inclusion of affected people.

However, whether we use FSPs will depend on several factors – what people prefer / are comfortable with, what financial services exist, and the potential risks for the affected populations. This brief focuses on the latter, specifically, data protection-related risks – by understanding what personal data and how that data is generated and/or shared, we will be better equipped to assess the risks surround data protection.

UNDERSTANDING THE FSP DATA FLOW

When working with or through FSPs, it is important to first understand the "general picture". Without understanding where personal data is created or collected, or where it has to go, it is difficult to analyse and assess the risk. To map out the processes and the routes that the data takes, it is therefore helpful to draw a representation of the system, often called a "data flow diagram". It portrays the combinations of data flow that can happen in a represented system.

Understanding the data flow helps us to identify the critical parts of the system and see the potential risks in relation to the personal data and further meta-data the system could generate. The risks associated will vary from uninformed consent to marketing / services unrelated to humanitarian assistance to potential threat to safety and/or dignity in humanitarian situations as a result to beneficiary screening, profiling, or other targeting/discriminatory practices.

Each context and FSP will offer its own set of unique services and processes. These services and processes might generate their own new data flows which, while they might not be necessary for the primary humanitarian purpose, might constitute a legal obligation for the FSP and, therefore, impossible to avoid. Within the scope of CVA and from the perspective of the affected person, we should try to understand where these data flows happen, whether they are likely to create additional risks, and what the mitigating options are.

	Primary interactions	**Secondary interactions**
Affected person	ICRC • Recipients will typically provide personal data to ICRC during registration and assessment • ICRC is responsible to collect data only as needed and ensure they are protected while it implements its activities including further analysis of the data	FSP • ICRC may have to share with FSP some personal data in order to create the recipient account and/or make the financial transfer. We should always share only the data that is strictly necessary for this purpose, and nothing more.
	FSP • Recipients may sometimes have to engage directly with the FSP to create an account. When recipients do not have an existing account, the ICRC may sometimes support the affected person in registering for an account. However, it is possible that they may	ICRC • The FSP will have to share financial reports to ICRC as proof of delivery. Some personal data may be included. Other vendors

[1] The term CVA can be used interchangeably with CTP "cash transfer programming", CBI "cash-based interventions" and CBA "cash-based assistance". In 2018 the wider humanitarian sector took the decision to use the term CVA "Cash and voucher assistance" as being the clearest descriptor of what this is all about. Previously ICRC used CTP but will now use CVA to be in line with the wider humanitarian sector. (So, don't worry if you see older documents using the term CTP…it's the same thing as CVA!)

	already have an existing account. When the affected person has an existing account, we should strive to ask their preference (use existing / create a new account). • The registration process for financial services typically requires personal data including bringing a form of identity document.	• It is possible that the FSP may share personal data to other suppliers for commercial / marketing / other purposes. Where ICRC's Standard Terms & Conditions are accepted by the FSP, this is forbidden without the prior written agreement of the ICRC. Regulatory body • Bound by national regulatory laws, the FSP is likely obligated to screen the recipients as part of its Know Your Customer (KYC) and Anti Money-Laundering (AML) policies and, potentially, to notify authorities in case of a positive match.
	Person / Merchants / Agent • Recipients may transfer money to another person, purchase directly from merchants, and/or cash-out through agents / branches. • All these interactions may generate meta-data on these transactions like the geolocation, time stamp, and amount withdrawn / spent.	FSP • Meta-data generated is recorded and shared with the involved FSPs

Below is a data flow diagram which illustrates a typical FSP system which shows where data is generated and/or shared. Your context might engage in only some or all of these processes (or have others that are not depicted here). Fully recognizing that protection risks, including from a data protection perspective, are complex and continuously evolving, we try to frame the risks we are trying to mitigate. By understanding how the data is likely to flow, we can see where the risks may lie and determine the appropriate mitigating measures.

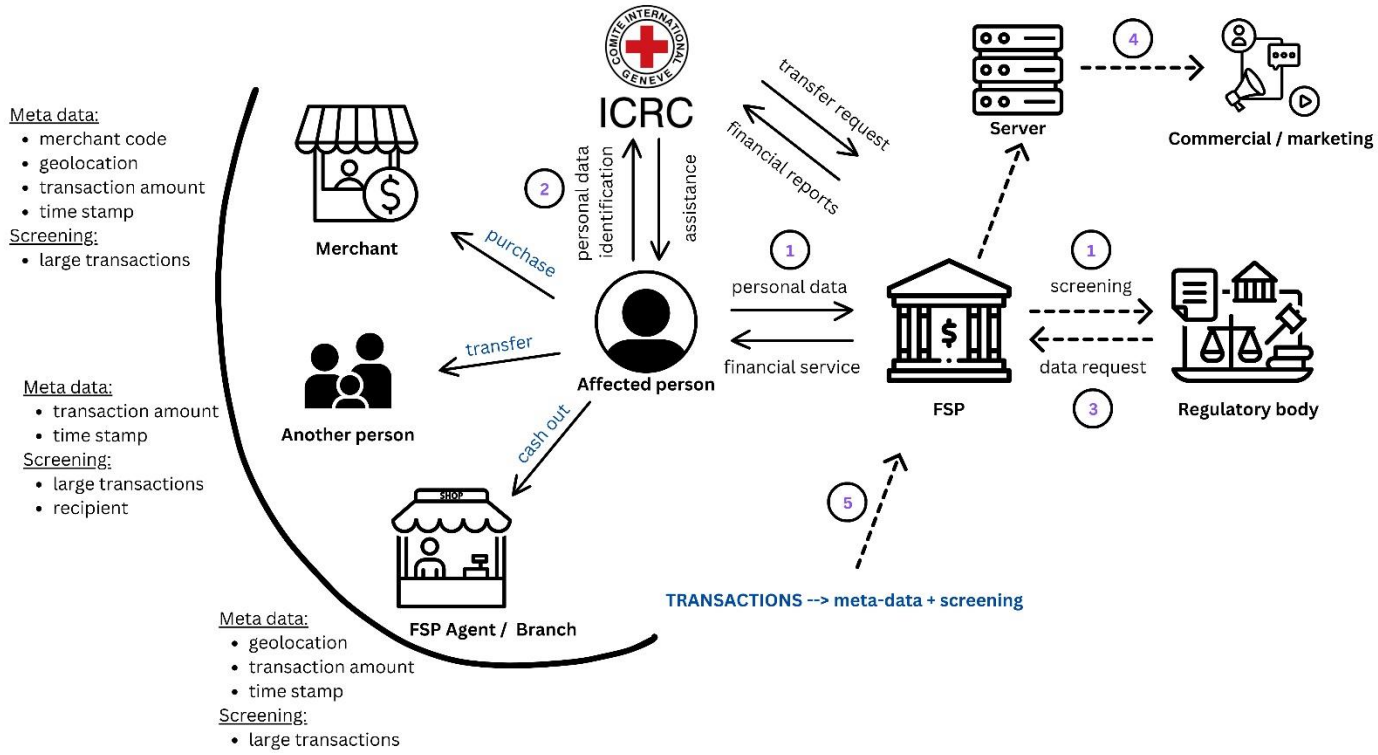

Figure 1. A typical data flow for cash assistance

# in Fig.1	Challenge	Potential risk	Mitigating measures
1	**Sanction screening** This is likely at account opening, during transactions, and/or at set intervals set by the FSP. Either transactions and/or names are screened against sanctions list to flag suspicious activities typically related to funding terrorism and/or money laundering.	The risk of potential exposure of a person in case of a positive or false positive matches during this screening process and if the FSPs are required to report to the regulatory body. This means that should they find a person who has been included in a terrorist list or subject to sanctions, the FSP might have a legal obligation to report them to the relevant authorities, notably security agencies, with the inherent risk of subsequent investigations and prosecutions.	• During the feasibility study, consultation with the community, and/or during individual registration, asses whether people are already engaging with financial products and services themselves. If so, it is likely that they have already been screened before and may provide indication whether there has been issues before or not for this community / population group. • Try to ensure that affected populations have true understanding of what this process entails, including potential transfers to third parties. They should also be provided for the opportunity to voice any concerns they may have on the process. This is often challenging to communicate, wherever possible, use simple language and ensure that people don't feel obliged to agree to their data being shared to an FSP out of fear of exclusion from assistance. • Always prepare an alternative form of assistance, whether that means direct cash in envelope (if feasible); or providing assistance as an in-kind equivalent and/or direct service. • Try to understand the country's laws and regulations which typically includes counter terrorism regulations and sanction regimes (including lists of designated individuals and entities). Individuals or target populations who may be at risk may be offered an alternate form of assistance which doesn't involve an FSP.
2	**Assistance exclusion due to FSP requirements** As we work with the most vulnerable populations there may be barriers to engage with the FSP due to lack of formal identification requirements needed to create an account	The risk of such requirements posed by the FSP may lead to a misconception that the affected person may feel that they would be excluded from assistance.	• Always prepare an alternative form of assistance, whether that means direct cash in envelope (if feasible); or providing assistance as an in-kind equivalent and/or direct service.

	and/or if they identify as an 'at risk' group in which sanction screening poses a risk to the individual.		
3	**National legislation may require FSP to disclose data** As FSPs are subject to their national legislation, they may have to oblige in disclosing data should the authorities request it.	This risk is similar to risk 1 such that data may need to be shared should it be requested by the authorities in a legal proceeding. The risk of potential exposure of a person in case of a positive or false positive matches during this screening process and if the FSP are required to report to the regulatory body. This means that should they find a person who has been included in a terrorist list or subject to sanctions, the FSP might have a legal obligation to report them to the relevant authorities, notably security agencies, with the inherent risk of subsequent investigations and prosecutions.	• Try to understand the country's laws and regulations which typically includes counter terrorism regulations and sanction regimes (including lists of designated individuals and entities). Individuals or target populations who may be at risk may be offered an alternate form of assistance which doesn't involve an FSP (eg direct cash, in-kind, direct service). • If such disclosure is a legal obligation accruing to the FSP, there is very little the ICRC can do to mitigate the risk and impact. It is therefore essential, before contracting with the FSP, to assess the scope of such obligations, if applicable, and their potential effect vis-à-vis the target population. Should the risks outweigh the benefits of such operation, contracting with the FSP in question should be excluded at the outset, and alternative solutions be found. Include a contractual obligation for the FSP to notify the ICRC in advance of any disclosure, so that the ICRC may take the necessary steps to address the situation, including invoking its privileges and immunities, where applicable.
4	**Processing for further (incompatible) purposes**	Typically, personal data will be needed for the FSP to execute the transfer we requested. However, using personal data for a purpose other than that for which they were initially collected should be avoided. This includes for commercial purposes or anything else not clearly mentioned in the Framework Agreement.	• Where ICRC's Standard Terms & Conditions are accepted by the FSP, this is forbidden. If the standard contract is not accepted, try to contractually negotiate for exclusion of any unnecessary further processing to minimize the non-humanitarian services so that we have data minimization / purpose limitation with logistics and DPO.
5	**FSP and other intermediaries are able to track individuals through their transactions / metadata**	All transactions generate metadata about the individual and their activities. This information is visible to the FSP, but also to the local / international / multinational companies that provide the infrastructure the service relies upon (network, telecomunication, mobile,	• Where this risk can have significant impact, recommend beneficiaries to exchange in hard currency as often as possible, only to use ATM / FSP services to restock on money.

	cloud providers, other third parties that the FSP might rely upon). Though this is an inevitable consequence of the service and very little can be done about, it must always be in the minds of CVA operators and other humanitarian workers that any digital system leaves traces and what is called a "digital footprint"	• Inform individuals about this risk so that they can be aware of their digital footprint

RISKS AND MITIGATION

Knowing that risks can never be completely eliminated and acknowledging that financial transactions are part of people's day-to-day activities, we should still do our utmost to ensure that people's personal data are protected and when data needs to be shared, it is as minimal and only as necessary as possible. The potential risks will vary depending on the payment solution and the functionalities it offers and not all risks are equal.

Understanding the general flow of data through an FSP helps us understand and assess better the type of risks that is relevant and where these data transfers happen. Although we can never eliminate all risk, this helps determine whether the risk identified is acceptable with the right mitigating measures or not at all.

One of the added values of cash assistance is that it provides more choice, dignity, and agency to the affected person. It is thus essential to ensure that we include the affected people in the discussion and response option analysis and not decide unilaterally on their behalf. Data protection considerations allow us to frame the discussion in a coherent manner, ensuring on the one side that applicable regulatory requirements are complied with, while at the same time guaranteeing that no further harm is done by using external providers.

CONCLUSION

Understanding the general flow of data through an FSP helps us understand and assess better the type of risks that is relevant and in which transactions these risks occur. Although we can never eliminate all risk, this helps determine whether the risk is acceptable with the right mitigating measures or not at all for a given group of beneficiaries.

In particular, screening risks "real world" harm to some beneficiaries, but not using cash transfers where appropriate, including through FSPs, reduces the effectiveness of our response and has a reputational risk with affected people and donors. However, risks will be person and context specific. For example, the risk of screening to released detainees and/or their families in some contexts may be higher than the general civilian population. And of course, we don't have to use FSPs, we can assist people in other ways through direct cash in envelope by the ICRC or giving in kind assistance. In fact, based on the NIIHA principles, we must always have alternative ways to provide assistance to those in need including if there are risks / barriers that prevents them from receiving cash transfers.

GLOSSARY

Anti Money Laundering (AML) refers to legally recognized rules for preventing money laundering.

Consent means the freely-given, specific and informed indication of a Data Subjectt's wishes by which the Data Subject signifies agreement to Personal Data relating to him or her being processed.

Data Breach means the unauthorized modification, copying, unlawful destruction, accidental loss, improper disclosure or undue transfer of, or tampering with, Personal Data.

Data Controller means the person or organization who alone or jointly with others determines the purposes and means of Processing of Personal Data.

Data Processor means the person or organization who processes Personal Data on behalf of the Data Controller.

Data Protection Impact Assessment or DPIA means an assessment that identifies, evaluates, and addresses the risks to Personal Data arising from a project, policy, programme or other initiative.

Data Subject means a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Perosnal Data.

Further Processing means additional Processing of Personal Data that goes beyond the purposes originally specified at the time the data were collected.

Know Your Customer (KYC) is a process enabling businesses to check the identity of their customers in order to comply with regulations and legislation on money laundering and corruption.

Personal Data means any information relating to an identified or identifiable natural person.

Processing means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination or erasure.