Orientação Prática para a Proteção de Dados na Assistência Monetária através de Vouchers

Complemento do Kit e Ferramentas de Assistência Monetária em Situação de Emergências

Janeiro de 2021

Índice

I. Introdução

À medida que o Movimento Internacional da Cruz Vermelha e do Crescente Vermelho implementa os seus compromissos de ampliar a Assistência Monetária e através de Vouchers (AMV), também aumenta a recolha e o tratamento de dados pessoais, em particular das comunidades vulneráveis que recebem os serviços. A proteção de dados não é somente um assunto de boa governação; também deve gerar confiança. Em tempo de crise, os beneficiários podem ter prioridades necessárias mais urgentes para a sua sobrevivência e segurança do que os riscos dos seus dados pessoais fornecidos a organizações assistenciais. Este é um motivo ainda mais importante para os profissionais da assistência monetária respeitarem e se responsabilizarem pela proteção dos dados dos beneficiários. Adicionalmente, outras partes interessadas, tais como doadores, entidades governamentais e outros sócios, terão maior confiança nos nossos programas de AMV se boas normas e práticas de proteção de dados forem demostradas.

Público-Alvo e Objetivo do Documento

A presente orientação prática é destinada aos **profissionais da assistência monetária** ou àqueles que geram programas para a integração dos princípios de proteção de dados na implementação da AMV. Há muitas referências de proteção de dados úteis disponíveis para os atores humanitários, incluindo o Manual sobre Proteção de Dados na Ação Humanitária e as respetivas políticas de Proteção de Dados da FICV e do CICV. Enquanto essas referências têm uma natureza mais geral ou somente tratam algumas das questões que os profissionais da assistência monetária têm de confrontar num nível elevado, o presente documento visa traduzir os princípios gerais de proteção de dados numa orientação prática, aplicável e específica das atividades principais no processo da AMV. Esta orientação fornecerá considerações essenciais sobre a proteção de dados e orientará os profissionais da assistência monetária na tomada e implementação de decisões.

Este documento faz referência aos processos no *Kit* de Ferramentas de Assistência Monetária em Emergências (AMeE) e vai complementar o *kit* de ferramentas até a sua revisão para incluir diretamente as considerações de proteção de dados explicadas neste documento.

IMPORTANTE:
Esta orientação deve ser contextualizada pelas Sociedades Nacionais para cumprir os próprios requisitos; em particular, o cumprimento das suas leis e políticas nacionais de proteção de dados, que podem ser mais estritas do que o padrão de proteção de dados aplicado aqui.

Estrutura do Documento

O próximo capítulo fornecerá uma análise geral da Proteção de Dados para introduzir os leitores aos principais princípios e terminologias que vão ser usados na orientação. Será seguida de um capítulo para cada um dos cinco processos essenciais da AMV.

Antes da elaboração desta orientação, foi realizada uma análise do *kit* de ferramentas de AMeE para identificar os processos nos quais os dados pessoais dos beneficiários são recolhidos e tratados. Depois, os processos são priorizados em função do nível de tratamento dos dados pessoais e dos riscos potenciais. Esta orientação focalizará em cinco desses processos prioritários[1]:

1. Direcionamento
2. Registo dos beneficiários
3. Uso de Fornecedores de Serviços Financeiros
4. Partilha de dados com Governos, outras Organizações Humanitárias e Doadores
5. Monitoramento após a Distribuição

[1] Este documento visa ser um documento dinâmico, e poderá ser desenvolvido uma orientação prática para outras áreas do *kit* de ferramentas de AMeE em revisões subsequentes à medida que adquirimos experiência em proteção de dados.

Cada capítulo incluirá uma análise geral que descreverá como se utilizam ou tratam os dados pessoais, com exemplos baseados nas consultas com as Sociedades Nacionais. Será seguido de um conjunto de considerações de proteção de dados baseados nas decisões ou questões essenciais dos projetos.

Cada consideração começa com um quadrado que destaca uma decisão ou questão essencial de um projeto. Um ícone de campainha indica quais são os princípios de proteção de dados relevantes para a consideração. Depois, um enquadramento da respetiva pergunta do projeto é fornecido para a incorporação da consideração de proteção de dados. Essas considerações são explicadas de forma detalhada e acompanhadas por exemplos simplificados para demostrar como aplicar as considerações.

O último capítulo trata as Considerações Gerais aplicáveis para todo o ciclo do programa da AMV.

II. Análise Geral da Proteção de Dados

Tratamento de Dados Pessoais

O que são exatamente os dados pessoais? Os **dados pessoais** são qualquer informação que possa levar à identificação de uma pessoa viva e singular (a pessoa em causa). Os dados podem ser pessoais, mesmo que à primeira vista possa parecer que não estão vinculados diretamente a uma pessoa, pois podem levar à identificação indiretamente através do uso de informação adicional. Pode parecer complicado, mas basicamente significa que a proteção de dados abrange um vasto conjunto de informações, e que o termo "dados pessoais" não deve ser interpretado num sentido restrito. No contexto da AMV, a maioria dos dados recolhidos dos beneficiários qualificam como dados pessoas, por exemplo:

- Nomes e dados do contacto;
- Números de identificação;
- Números da conta bancária;
- Dados do emprego;
- Situação familiar;
- Estado de saúde;
- Endereço ou geolocalização;

Pelo contrário, os dados recolhidos para analisar a situação a **nível abstrato** (por exemplo, informação económica sobre a região, etc.) não qualificam geralmente como dados pessoais. Esses dados são anónimos, porque não tratam de modo algum com informação pessoal, ou porque a informação está em forma agregada. Os **dados agregados** são dados criados por meio da síntese e combinação de dados individualizados. As pessoas singulares não são identificáveis através dos dados agregados (nem direta nem indiretamente), que geralmente fornecem uma análise geral através de gráficos, tabelas, estatísticas e informação geral sobre grupos de pessoas, não sobre pessoas singulares. Exemplos disso incluem estatísticas sobre tipos de sustento, dimensão ou renda média dos agregados familiares, percentagens de danos aos abrigos numa área, ou o cálculo do cabaz mínimo de despesas.

O **Tratamento** de dados pessoais refere-se essencialmente a qualquer coisa que seja feita com os dados, como a recolha, conservação, organização, partilha, avaliação, alteração, publicação, registo, uso, correção e até a eliminação.

Base Legítima

Todo tratamento de dados pessoais exige uma base legítima (ou *legal*). Uma base legítima comumente usada é o consentimento. No entanto, existem várias outras bases para legitimar o tratamento de dados pessoais, incluindo:

- Cumprimento de uma obrigação legal;
- Execução de um contrato com a pessoa em causa;

- Uma tarefa no interesse público;
- Interesse ou interesses vitais de uma pessoa (ameaça a curto prazo para o estado mental ou físico);
- Interesse legítimo da entidade (pode ser a FICV, o CICV, a Sociedade Nacional, por exemplo) que realiza o tratamento dos dados pessoais;

A questão da base legítima na qual se baseau, pode ser desafiadora. Mais detalhes sobre a definição e as diferenças dessas bases legítimas na Política da FICV sobre Proteção de Dados e no Manual sobre Proteção de Dados na Ação Humanitária do CICV e do Centro de Privacidade de Bruxelas.

Para a AMV, é bastante comum usar a base do consentimento. Muitos profissionais da assistência monetária incluem uma pergunta sobre o consentimento ao início de uma pesquisa ou de um formulário de recolha de dados. No entanto, para as emergências, essa não é necessariamente a melhor opção. Esta questão explica-se com mais detalhe no capítulo sobre o Registo de Beneficiários, com uma árvore de decisão para ajudar a avaliar se uma ou várias bases legítimas podem ser mais apropriadas nas circunstâncias existentes.

Princípios Essenciais na Proteção de Dados

Há vários princípios de proteção de dados para considerar no processo de tratamento de dados pessoais. Embora os nomes possam mudar em função da política ou do instrumento internacional, é geralmente aceite que os principais princípios de proteção de dados são: (1.) licitude, lealdade e transparência; (2.) limitação da finalidade; (3.) minimização dos dados; (4.) exatidão; (5.) limitação da conservação; e (6.) integridade e confidencialidade (segurança). Mais detalhes sobre isso na Política da FICV sobre Proteção de Dados e no Manual sobre Proteção de Dados na Ação Humanitária.

No entanto, para efeitos desta orientação, vamos focalizar nos princípios mais relevantes para a AMV (indicando que o princípio de licitude, ou a "base legítima", já foi discutido acima). Com frequência, os princípios que devem ser considerados conjuntamente para fazer a análise de proteção de dados relevantes são discutidos conjuntamente, mesmo que em rigor sejam considerados princípios diferenciados. Por exemplo, na próxima seção discutiremos de forma conjunta dois princípios diferenciados, "minimização dos dados" e "limitação da finalidade", porque não é possível avaliar quais são os dados necessários sem fazer uma avaliação da ou das finalidades da recolha/tratamento de dados.

Minimização dos Dados, Necessidade e Limitação da Finalidade

O princípio de minimização dos dados significa "recolher o menos possível e SOMENTE o necessário". Para definir o que é necessário, é importante identificar claramente a *finalidade* do uso dos respetivos dados. No contexto da AMV, o tratamento de dados pessoais pode servir a várias finalidades (por exemplo, comprovação em relação aos critérios de direcionamento, comprovação da identidade, facilitação da distribuição monetária, para detetar ou evitar fraudes, e o monitoramento do impacto do programa). O tratamento de dados pessoais deve ser *necessário* para alcançar a respetiva finalidade. Antes de recolher a informação, é essencial compreender qual é a informação necessária no contexto específico. Se não tem certeza sobre qual é o motivo para recolher um conjunto particular de dados ou pensa que esses dados podem ser úteis posteriormente sem um motivo específico, ou simplesmente pensa que quanto mais dados sejam recolhidos dos beneficiários, melhor, é provável que vai recolher mais dados pessoais do estritamente *necessário*. Para identificar claramente quais são os dados necessários, aconselha-se a revisão dos princípios de minimização dos dados / necessidade / limitação da finalidade. Essas questões são essenciais para a proteção de dados e vão surgir com frequência nesta orientação. Mais detalhes e exemplos relevantes são fornecidos no capítulo de Direcionamento.

Além disso, os dados pessoais recolhidos para uma finalidade não podem simplesmente ser usados para qualquer outra finalidade. Naturalmente, um conjunto de dados pode ser usado para finalidades

futuras em certas circunstâncias. No entanto, as finalidades futuras devem ser geralmente "compatíveis" com a finalidade original. Essa compatibilidade existe quando as finalidades estão estreitamente ligadas, e pode ser presumido que a pessoa em causa não se surpreenderia desse uso secundário. Por exemplo, no final de um programa de AMV, se recebem fundos adicionais que não estavam previstos anteriormente. Uma revisão dos dados dos beneficiários anteriormente recolhidos para determinar quais são os beneficiários que devem receber uma nova assistência seria considerada compatível com a finalidade e a base legítima da anterior recolha de dados pessoais. De outra forma, se deveria identificar uma base legal apropriada e a pessoa em causa poderia ter de receber informação atualizada sobre o uso subsequente pretendido (ver princípio de Transparência abaixo).

Transparência

A transparência vai junto com a lealdade. A ideia é ser abertos e honestos no que diz respeito ao tratamento dos dados pessoais. Conforme o princípio de transparência, as pessoas em causa sempre devem receber certa informação essencial sobre o que está acontecer com os seus dados, incluindo:

- O facto de que os seus dados pessoais estão a ser tratados e a base para o tratamento;
- Quem fará o tratamento dos dados;
- Com que finalidade ou finalidades os dados estão a ser tratados;
- Como se devem conservar os dados e por quanto tempo;
- Se se pretende partilhar os seus dados com outra entidade;
- Os direitos no que diz respeito ao tratamento, como o direito à correção e à eliminação;
- Dados de contacto ou a quem recorrer se as pessoas em causa tiverem perguntas ou reclamações;

A forma na qual essa informação se fornece depende do contexto. Se fornecerão exemplos específicos ao longo da orientação.

Segurança dos Dados (Confidencialidade, Integridade, Limitação da Conservação) [2]

Os dados pessoais devem ser tratados em confidencialidade e com segurança. Isso pode ser óbvio, mas o que deve ser feito para garantir a confidencialidade não é sempre claro. A lei (ou a política, se aplicável) de proteção de dados exige a implementação de várias medidas de segurança, como as restrições do acesso e a prevenção da perda dos dados. O objetivo último é evitar violações de dados, o que significa *o acesso não autorizado a dados pessoais ou a sua destruição, perda, alteração ou divulgação*.

III. Direcionamento

Uso de Dados Pessoais

O direcionamento da assistência monetária é estabelecido pelos objetivos do programa em função das necessidades avaliadas. Alinha as atividades do programa com os beneficiários específicos através de critérios de direcionamento definidos, que geralmente incluem indicadores socioeconómicos e de vulnerabilidade. Ver seção M3_3 do *kit* de ferramentas de AMeE para mais detalhes.

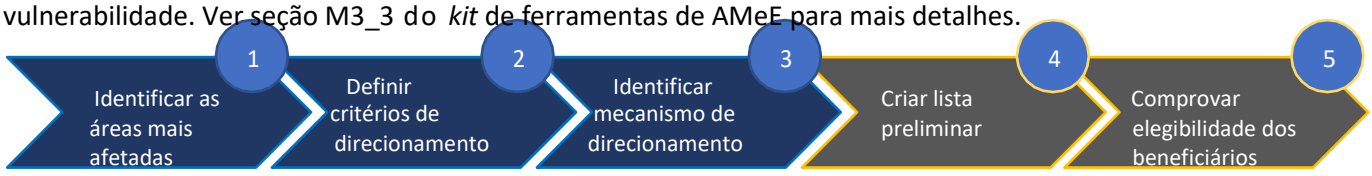

Figura 1: Passos no processo de direcionamento

Os passos gerais no processo de direcionamento mostram-se na *Figura 1*. Este processo pode basear-se em dados recolhidos anteriormente para sustentar o estabelecimento de critérios e acelerar a criação da lista preliminar dos beneficiários elegíveis para a AMV.

Os passos 1 a 3 abrangem as decisões essenciais de direcionamento de acordo com os objetivos do programa. Essas decisões incluem:

[2] A limitação da conservação considera-se geralmente um princípio diferenciado.

- Quais as localizações geográficas selecionadas para a intervenção?
- Distribuições globais ou dirigidas?
- Dirigidas a agregados familiares ou a pessoas singulares?
- Quais são os critérios de direcionamento que se devem escolher em função dos elementos de vulnerabilidade, socioeconómicos, ou específicos do contexto?
- Que mecanismo de direcionamento escolher (mecanismo de direcionamento categórico, de autodirecionamento ou de direcionamento baseado na comunidade)?

Em geral, os dados pessoais não têm um papel significativo nesses três primeiros passos. As decisões baseiam-se na informação geral ou em dados agregados das áreas afetadas e na população em geral. Aqui a situação individual dos potenciais beneficiários não é ainda de interesse, mas sim a situação global no terreno e os objetivos do programa.

No entanto, os passos 4 e 5 lidam sim com os dados pessoais, pois os potenciais beneficiários são analisados e comprovados em relação aos critérios estabelecidos, e uma lista preliminar de beneficiários é criada antes do processo formal de registo de beneficiários. A lista terá pelo menos os nomes dos beneficiários, e o processo de análise ou verificação poderá ainda conter informação detalhada sobre os beneficiários.

No Passo 4, a lista preliminar desenvolve-se geralmente de acordo com o mecanismo de direcionamento estabelecido no Passo 3:

- **Direcionamento baseado na comunidade** – famílias vulneráveis identificadas por líderes e membros comunitários em função dos critérios acordados; os resultados são triangulados e comprovados pela Sociedade Nacional. Por exemplo, solicita-se aos líderes comunitários para identificarem as famílias com residências completamente destruídas.
- **Autodirecionamento** – solicita-se às pessoas singulares para fornecerem informação sobre elas mesmas e detalhes ligados aos critérios acordados. Por exemplo, a equipa do programa procura adultos em situação de insegurança alimentar e fisicamente aptos dispostos a participar num programa de Dinheiro em troca de Trabalho.
- **Direcionamento categórico** – a elegibilidade baseia-se em categorias específicas de vulnerabilidades (por exemplo, famílias chefiadas por crianças) e potencialmente num bom registo civil para decidir que pessoas singulares pertencentes a uma categoria específica devem ser selecionadas. Por exemplo, solicita-se aos funcionários governamentais para partilharem uma lista de membros comunitários na pobreza extrema.

Independentemente do mecanismo de direcionamento usado, esse passo baseia-se em dados recolhidos de diferentes fontes (tais como o governo, comunidades locais, outras organizações ou pessoas singulares). Embora a lista inicial possa ser obtida de outra fonte, o ato de receber essa lista já qualifica como uso de dados pessoais. Se não tiver uma lista inicial disponível, a Sociedade Nacional pode optar por ir de porta a porta nas comunidades afetadas para elaborar essa lista solicitando dados pessoais.

No Passo 5, comprova-se a elegibilidade de todas as pessoas nomeadas na lista preliminar. Este processo pode envolver representantes comunitários ou líderes locais com conhecimento da população ou que tenham informação estruturada através de outros dados ou sistemas (por exemplo, registo civil ou listas de proteção social). Nalguns casos, a Sociedade Nacional pode ir de porta a porta para comprovar diretamente com os beneficiários que efetivamente são elegíveis de acordo com os dados pessoais fornecidos. O processo dessa comprovação pode fazer-se em paralelo à criação da lista inicial de acordo com o Passo 4. Este processo de verificação pode ser similar ao processo de registo de beneficiários e pode usar formulários de pesquisa e uma base de dados para recolher e gerir dados pessoais estruturados ou pode fazer-se *ad hoc* somente com uma caneta e um papel para marcar os critérios

cumpridos pelo beneficiário; isso considera-se também dados pessoais.

No final do processo de direcionamento, a lista de beneficiário verificada pode ser partilhada e publicada na comunidade (por exemplo, a lista é impressa e publicada num espaço público para a comunidade comprovar quem está incluído na intervenção). A publicação dessa lista qualifica como uso (tratamento) de dados pessoais, pois envolve tornar dados sob o seu controlo acessíveis a outros – a todos os membros da comunidade, para que possam avaliar a lista.

Considerações de Proteção de Dados

O processo de direcionamento envolve o tratamento de dados pessoais no estabelecimento da lista preliminar de beneficiários e na comprovação dessa lista. Esta seção examinará decisões essenciais de projetos no processo de direcionamento e as considerações ligadas à proteção de dados. O princípio mais relevante tratado por esta seção é a **minimização dos dados/necessidade**. Todos os outros princípios referem-se ao tratamento dos dados recolhidos, enquanto a minimização dos dados e a necessidade visam a limitar a recolha de dados à partida. Não recolher os dados que realmente não sejam necessários para o programa é a forma mais efetiva para aumentar o nível de proteção de dados. Assim, ao estabelecer o programa e antes de recolher qualquer dado sobre os beneficiários, é essencial refletir sobre o ciclo de vida do programa e decidir com antecedência quais são os dados que serão necessários ao longo do programa.

Decisão do Projeto 1: Devo usar dados de beneficiários recolhidos por uma fonte exterior?

🔔 Minimização dos Dados, Necessidade e Segurança dos Dados

Decisão do Projeto reformulada: Será que eu preciso dos dados recolhidos por uma fonte exterior e como posso garantir que os dados do beneficiário foram recolhidos de forma apropriada?

Na criação da lista preliminar de beneficiários, é comum usar dados dos beneficiários procedentes de fontes exteriores, como outras organizações ou o governo. Por isso, a pergunta sobre a decisão do projeto pode parecer óbvia e necessária. No entanto, a pergunta sobre a decisão do projeto reformulada aconselha aos profissionais da assistência monetária tomarem uma abordagem matizada para solicitar e usar dados de fontes exteriores que tenha em consideração os princípios de minimização dos dados e de segurança dos dados, em particular quando não estiver estabelecido nenhum acordo de partilha de dados.

Aqui estão alguns elementos essenciais para considerar quando se contemple o uso de dados de beneficiários recolhidos por fontes exteriores (outras organizações não governamentais, Governo, etc.):

- **Será que esta organização é fiável e que eu posso confiar nos seus dados?** Se a organização que oferece os dados não é reconhecida, pode ser aconselhável perguntar ou investigar como foram recolhidos os dados e se isso pode ser considerado fiável. Nesse caso, a questão não é somente que os dados possam estar incompletos ou ser incorretos, mas também que é possível que os dados foram obtidos de forma inapropriada (por exemplo, sem uma base legal clara ou sem que os beneficiários tenham sido informados sobre como os dados deles serão partilhados com outros, particularmente se os dados são muito sensíveis). Em função do contexto, seria útil perguntar a líderes comunitários ou a outras organizações ativas na área se conhecem e confiam nessa organização. Também é aconselhável pedir para a organização fornecer alguma informação sobre como foi feita a recolha. É importante saber se os beneficiários têm conhecimento que os seus dados podem ser partilhados com outros. O facto

de outro tiver dúvidas se tudo isso foi feito de forma apropriada é um indicador de que pode ser aconselhável considerar outras fontes de dados.

- **Que dados devo solicitar e aceitar?** O facto de outra organização ter recolhido uma certa quantidade ou tipos de dados, não significa que você deve tomar **todos nem a maioria** deles. De novo, é bom refletir nos princípios de minimização e dados e da necessidade. Depende do projeto quais dados devem ser solicitados ou aceites. Se a outra organização fornece-lhe mais dados dos que precisa, é aconselhável solicitar unicamente aqueles dados, e se são fornecidos dados desnecessários, elimine esses dados e informe a outra organização para que tenha conhecimento de quais dados foram utilizados. Recomenda-se também ter precaução se o conjunto de dados contém categorias de dados muito sensíveis, tais como: informação da saúde, sexual ou religiosa, em particular se esses dados não forem diretamente relevantes para as necessidades do programa. O facto de uma organização fornecer livremente esses tipos de dados com ou sem um acordo formal de partilha de dados pode indicar que as suas normas de proteção de dados são fracas ou inexistentes. Além disso, os dados recebidos de entidades externas devem ser tratados de forma responsável.

O cenário descrito acima não envolve contratos de partilha de dados entre as partes e, portanto, o controlo dos dados torna-se uma consideração importante. Para os programas de AMV nos quais a Sociedade Nacional é um sócio implementador de outra agência, a partilha de dados deve ser acordada entre as entidades envolvidas, sejam externos ou outros, e essas considerações podem ser avaliadas na negociação do acordo de partilha de dados. Se, no contexto desses programas monetários, estiver preocupado com a proteção de dados no que diz respeito à partilha de dados com entidades exteriores, deve comunicar as suas preocupações ao diretor ou a equipa legal de sua Sociedade Nacional e registar os riscos/preocupações na matriz de riscos da AMV.

Exemplos:

O critério-alvo é "famílias com crianças que perderam a sua casa na enchente".

A equipa da Sociedade Nacional faz um pedido ao governo local para fornecer:

- "Informação relevante" sobre os residentes da área. Esse pedido é muito amplo, e é provável que o governo forneça mais informação do que a necessária. Esse pedido deve ser restrito.

- "Os nomes e a situação familiar de todos os residentes das áreas afetadas". Esse pedido é mais específico, mas ainda amplo demais. As pessoas sem crianças não fazem parte do alvo. Portanto, é improvável que os seus nomes sejam necessários.

- "Somente os nomes dos residentes nas áreas afetadas que tenham crianças". É provável que isso seja o necessário e suficiente.

Na sequência de um terremoto, a Sociedade Nacional tenta identificar as pessoas que perderam a sua casa. Uma associação da vila mais afetada oferece partilhar uma lista de pessoas que estão atualmente sem abrigo devido ao terremoto. A Sociedade Nacional considera essa oferta com atenção. Entra em contato com o prefeito da vila e pergunta sobre a reputação da associação. Além disso, entra em contacto com a associação para perguntar sobre o seu procedimento de recolha de dados. A associação explica que informou as pessoas sobre a proteção de dados e sobre a intenção de partilhar os dados com outras organizações de assistência. Os dados recolhidos pela associação incluem nomes, dimensão da família, idade das crianças e um número de telefone. A Sociedade Nacional planeia uma distribuição global para todas as famílias que perderam a casa. Em consequência, decide que, para a sua intervenção, somente precisa dos nomes dos beneficiários e dos números de telefone para entrar em contacto com eles. A equipa assegura-se de receber somente esses dados.

Decisão do Projeto 2: Como verificar a elegibilidade dos beneficiários?

Minimização dos Dados, Necessidade, Confidencialidade

Decisão do Projeto reformulado: De quais dados realmente preciso para verificar a elegibilidade dos beneficiários?

O objetivo da verificação ou a "comprovação de elegibilidade" é averiguar se uma pessoa (ou agregado familiar) realmente cumpre os critérios-alvo. Isto faz-se geralmente no **Passo 5** do processo de direcionamento mencionado acima, onde pode ser necessário recolher ou analisar dados ligados ao beneficiário. Ao realizar essa verificação, é importante não recolher nem tratar mais dados dos que sejam necessários para completar a tarefa (princípio de minimização dos dados e da necessidade). Diferentes métodos podem ser usados para comprovar a elegibilidade, que podem requerer ou tratar os dados pessoais de forma diferente:

- **Uso de membros comunitários para a verificação.** Nesse método, é possível ainda não consultar diretamente os beneficiários efetivos. Membros comunitários com conhecimento da situação ou dos dados pessoais dos beneficiários podem proporcionar uma lista preliminar de beneficiários potencialmente elegíveis. Isto pode ser seguido de uma comprovação mais formal durante o processo de registo de beneficiários. Com esse método, é importante que a privacidade dos beneficiários seja protegida, em particular se o método se realiza num contexto público (ou seja, com outros membros da comunidade) e dado que os beneficiários efetivos não podem se opor à partilha de informação que outras entidades já conhecem sobre eles. As perguntas dos líderes comunitários sobre os dados dos beneficiários devem ser minimizadas e as perguntas sensíveis devem ser evitadas num contexto público. Se quaisquer informações que poderiam ser consideradas sensíveis são necessárias para o programa, é preciso tentar recolher essas informações unicamente num contexto privado, por exemplo numa comprovação de porta a porta.

- **Comprovação de porta a porta.** Antes de visitar o agregado familiar beneficiário para comprovar a sua elegibilidade, é importante identificar quais dados são absolutamente necessários para esse fim, respeitando o princípio da minimização dos dados e da necessidade. Já que o esforço de ir de porta a porta pode ser elevado, pode existir a tendência a solicitar mais informações das estritamente necessárias, a fim de evitar ter de repetir a visita. Portanto, é essencial a preparação no tocante ao âmbito e à finalidade do programa, para solicitar somente o mínimo necessário para a verificação. Se não tiver certeza se uma certa informação deve ser solicitada, pergunte-se o seguinte: que impacto vai ter a informação na decisão de visar o beneficiário individual? Se não tiver certeza, é possível que não seja necessária.

- **Publicação da lista preliminar de beneficiários.** Como parte do Passo 4 ou após o Passo 5 do processo de direcionamento indicado acima, a lista preliminar de beneficiários é compartilhada e publicada num espaço público (tal como um salão comunitário). Faz-se isso a fim de gerar transparência e informar à comunidade sobre quem foi selecionado de acordo com os critérios de direcionamento acordados. Isso também oferece a oportunidade para aqueles que não estejam na lista, mas cumprem os requisitos de direcionamento de serem incluídos no programa. Essa lista contém dados pessoais e, portanto, é importante minimizar quais dados são compartilhados publicamente. Geralmente, é suficiente com os nomes e a localização geral, e não é necessário publicar os detalhes e dados usados na comprovação do direcionamento. Contudo, sabendo que a lista de nomes é ligada a alguns critérios definidos (mesmo que os detalhes de quais critérios são cumpridos ou não sejam mostrados), indica ao público em geral algum elemento sobre as pessoas na lista que pode ser problemático para a privacidade deles. O facto de isso ser problemático ou não do ponto de vista da proteção de

dados depende do contexto. Numa vila pequena na qual de qualquer forma as condições de vida de todos os residentes são de conhecimento geral, (quer dizer, que todo o mundo sabe se as pessoas têm ou não as características correspondentes aos critérios do direcionamento), a publicação da lista pode não ser tão problemática em termos de privacidade. Pelo contrário, num contexto no qual os beneficiários vivem em relativa anonimidade, a publicação da lista pode ser um problema. É provável que a divulgação de informações não conhecidas de forma pública anteriormente entre em conflito com o princípio de confidencialidade. Portanto, é aconselhável considerar atenciosamente o contexto antes de decidir se a lista deve ser publicada ou não.

Além disso, após a verificação ou o processo de comprovação de elegibilidade, os dados daqueles que não forem considerados elegíveis devem ser tratados de forma responsável (por exemplo, devem ser arquivados de forma segura se existem requisitos de auditoria, uma lista simplificada deve ser conservada, a fim de evitar uma nova verificação, ou eliminada se já não for necessária). Mais detalhes disso no capítulo de Orientação Geral.

Exemplos de necessidade e de minimização nas comprovações de elegibilidade:

No contexto de um programa, o critério de direcionamento é "famílias que cuidam de pessoas com incapacidade". Para a comprovação da elegibilidade, é necessário saber se realmente há membros com incapacidade que estão a morar no agregado familiar. Pode ser relevante conhecer o tipo de incapacidade que têm. Ao verificar os factos, isto será revelado durante a visita à casa, por exemplo. Contudo, provavelmente não seja necessário consultar os registos médicos para comprovar a incapacidade, e isso poderia revelar dados pessoais sensíveis que não sejam relevantes para o programa.

Os líderes comunitários sugerem visar como as mais vulneráveis as mães solteiras com pelo menos três crianças e sem renda, e uma lista preliminar é criada de acordo com esse critério. As informações fornecidas pelos líderes comunitários são verificadas nas visitas às casas, nas quais a beneficiária é identificada e perguntada sobre as idades de todos os membros da família. Para verificar a renda, pode ser necessário perguntar sobre as fontes de renda da beneficiária. No entanto, provavelmente não seria necessário recolher informações adicionais, tais como a idade ou a filiação religiosa, pois isso não vai influir na decisão de visar essa beneficiária. Também não é necessário perguntar sobre anteriores empregadores nem solicitar extratos bancários para determinar o nível de renda.

No contexto de uma resposta à fome, o critério-alvo para o programa monetário é "famílias chefiadas por crianças com insegurança alimentar". Na comprovação de elegibilidade, e improvável que seja necessário perguntar sobre o nível educativo das crianças. O nível educativo não vai influir na comprovação de elegibilidade nem na quantidade da subvenção monetária.

Nota: Na recolha de dados e em qualquer tratamento de dados, é importante lembrar que os dados pessoais devem ser tratados com segurança. Independentemente de se os dados forem recolhidos em papel, através de uma aplicação móvel ou de outros meios, é preciso garantir que os dados só são acessíveis para aqueles que estritamente precisem desse acesso. A segurança dos dados deve ser considerada em todas as fases, incluindo na sua eliminação, a fim de garantir que não possa ser recuperado. Mais detalhes disto no capítulo de Orientação Geral.

Decisão do Projeto 3: Devo falar com os beneficiários nesta fase sobre o tratamento dos seus dados?

Transparência

Decisão do Projeto reformulada: Como posso garantir que os beneficiários têm acesso a informação relativa ao tratamento dos seus dados?

Um princípio importante da proteção de dados é a Transparência. No contexto da comprovação de elegibilidade, a recolha de informação pode ser menos formal do que o registo dos beneficiários. No entanto, é importante os beneficiários saberem o que está ocorrer com as informações que compartilham consigo. Mais detalhes sobre como informar aos beneficiários são fornecidos no capítulo de Registo de Beneficiários, mas é bom cumprir com as seguintes normas quando fizer a verificação ou as comprovações de elegibilidade. Aqui alguns elementos sobre os quais informar o beneficiário:

- Onde conseguiu as informações principais sobre eles (por exemplo, através de membros comunitários, uma lista governamental, outras organizações?);
- O motivo pelo qual realiza a comprovação de elegibilidade;
- O facto de que os dados inexatos podem ser corrigidos em qualquer momento;
- O facto de que é possível que você compartilhe os dados fornecidos com outras instituições e com que finalidade (se for o caso);

IV. Registo de Beneficiários

Uso de Dados Pessoais

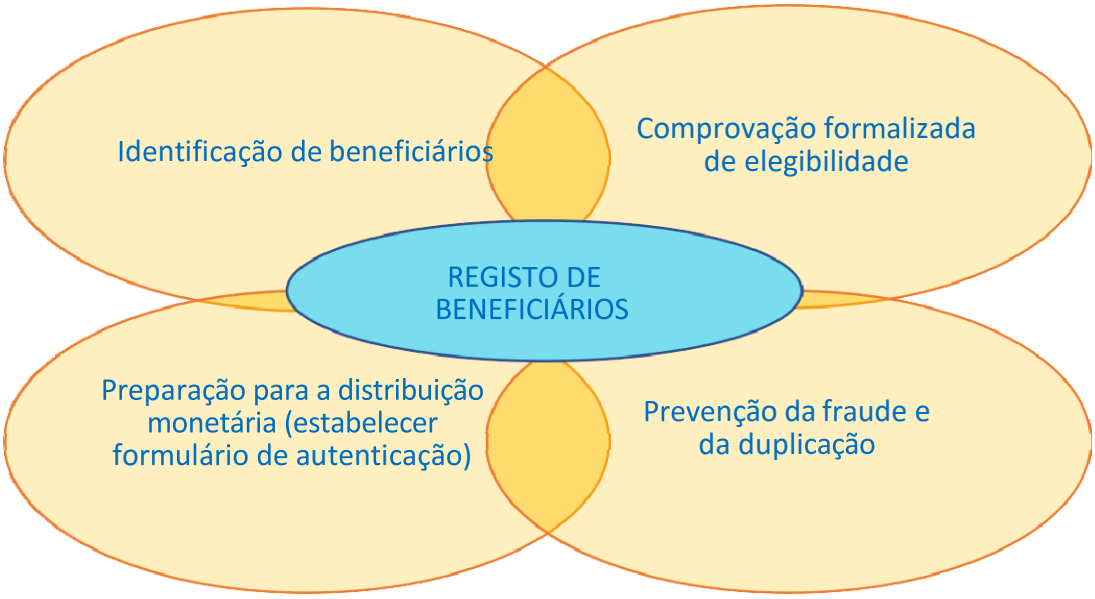

Figura 2: Finalidades para a realização do Registo de Beneficiários

O processo de registar formalmente os beneficiários ocorre geralmente após a criação de uma lista de beneficiários elegíveis (ver seção M4_4 do *kit* de ferramentas de AMeE para mais detalhes). Isto envolve a recolha de dados pessoais e a gestão desses dados para a distribuição e o monitoramento

do programa. A Figura 2 mostra as finalidades comuns do registo de beneficiários e os exemplos abaixo exemplificam o uso dos dados pessoais:

- **Identificação.** No início do processo de registo, solicita-se geralmente ao chefe de família para mostrar uma identificação (por exemplo, carta de condução, identificação fiscal ou de votação) para garantir que é a pessoa incluída na lista de beneficiários. Essas identificações contém o nome, a data de nascimento e outros dados pessoais que podem ser recolhidos no registo. Pode-se pedir ao beneficiário para fornecer dados biométricos (tais como a impressão digital) para uma sólida autenticação e a fim de garantir que sejam registados múltiplas vezes. Os dados biométricos são considerados dados pessoais e podem ser sensíveis.
- **Verificação formal da elegibilidade.** Fazem-se perguntas ao beneficiário relativas aos critérios de direcionamento se o processo de verificação não for feito formalmente antes, e se existir a possibilidade dos dados tiverem mudado desde que o direcionamento foi feito, a fim de comprovar antes do desembolso monetário que o beneficiário é ainda elegível.
- **Preparação da distribuição monetária.** Quando for aplicável, pede-se ao beneficiário a informação *Know Your Customer* (KYC) ou outras informações solicitadas pelo fornecedor de serviços financeiros (FSF) para a distribuição monetária (por exemplo, um número móvel para o dinheiro móvel ou os dados da conta bancária).
- **Estabelecer a forma de autenticação.** Um cartão de beneficiário da Cruz Vermelha é fornecido ao beneficiário com uma fotografia e um identificador único que poderá mostrar ao fornecedor de serviços financeiros como prova de que é elegível e foi registado. Isto é particularmente útil quando não existem identificações oficiais disponíveis.
- **Prevenção da fraude e da duplicação.** Para prevenir a fraude e a duplicação, pode-se pedir ao beneficiário que forneça dados pessoais relativos aos membros da família ou dados biométricos.

Considerações de Proteção de Dados

O processo de registo de beneficiários envolve a recolha e o tratamento dos dados pessoais em função das finalidades comuns descritas acima. Esta secção trata sobre as decisões essenciais do projeto no processo de registo e as considerações relativas à proteção de dados.

Decisão do Projeto 1: Como devo verificar a identidade do beneficiário?

🔔 Minimização de Dados, Necessidade

Decisão do Projeto reformulada: Que mecanismo de verificação é efetivo e interfere o menos possível com os interesses (incluindo a privacidade) dos beneficiários?

Para comprovar a identidade das pessoas que comparecerem ao registo, é preciso um identificador único. Os identificadores únicos podem ser em papel (carta de condução, cartão de identificação nacional, etc.) ou biométricos (impressão digital, leitura da íris, etc.). Ao considerar qual das opções usar, alguns aspectos operacionais devem ser considerados, mas a proteção de dados também. Nalguns contextos, solicitar cartões de identificação quando maioritariamente uma comunidade não tem esses documentos pode não ser muito útil. Em outros contextos, a recolha de dados biométricos pode parecer a maneira mais eficiente e a única de evitar a fraude. Numa perspetiva de proteção de

dados, é importante considerar que alguns dados são mais sensíveis do que outros. Sempre que for possível, o objetivo é recolher os dados menos sensíveis.

Identificação em papel

Em muitas áreas, a forma mais simples e comum é solicitar uma identificação, como um cartão de identificação nacional expedido pelo governo ou um passaporte. Solicitar esses identificadores não representa um risco elevado numa perspetiva de proteção de dados, já que esses documentos servem exatamente para a finalidade de identificar o titular. O facto de se for necessário digitalizar ou copiar e arquivar a identificação de cada beneficiário é uma questão aparte. Aos efeitos da identificação, com frequência é suficiente solicitar ao beneficiário para apresentar a identificação no registo e registar o número de identificação único. Pode marcar o quadrado de que a identidade foi comprovada sem conservar uma cópia íntegra da identificação. Identificações alternativas ou documentos tais como uma carta de condução, certidão de nascimento, certidão de batismo ou faturas de eletricidade, podem ser aceites em vez de uma identificação nacional se houver muitas pessoas na comunidade que não possuem essa identificação. Na recolha desses documentos, de novo recomenda-se recolher os menos dados possíveis para verificar a identidade. No contexto da proteção de dados, mais não é sempre melhor. Além disso, recomenda-se não solicitar documentação que contenha dados sensíveis (tais como documentos relativos à saúde). Também, tal como foi discutido, pode não ser necessário conservar cópias desses documentos.

Dados biométricos

Os dados biométricos são dados relativos às características fisiológicas ou comportamentais de uma pessoas reconhecidas por meios tecnológicos. Exemplos típicos disto são impressões digitais, digitalização da íris, digitalização das veias das mãos e reconhecimento facial e da voz. Esses dados são considerados muito sensíveis, já que são muito pessoais e não é uma coisa que possa simplesmente ser substituída se estiver em risco e, portanto, merecem um maior nível de proteção. Nalguns casos, os dados biométricos estão sujeitos a restrições legais, incluindo a limitação ou proibição de uso. O motivo principal para isso é o potencial uso indevido desses dados:

- **Aplicação da lei ou segurança.** Os dados biométricos podem ser muito interessantes para os atores da aplicação da lei ou da segurança, já que não podem ser alterados. Ao recolher esses dados no contexto de um projeto, pode estar exposto à pressão de outras partes para divulgar esses dados com outros fins.
- **Usurpação da identidade.** Os dados biométricos também são mais suscetíveis de serem hackeados para efeitos de usurpação da identidade, porque são únicos e não podem ser alterados.
- **Fonte de informação no futuro.** É possível que, no futuro, os dados biométricos recolhidos hoje possam ser usados para saber muito mais sobre uma pessoa do que é possível atualmente. Novas soluções tecnológicas podem ser capazes de obter mais informação deles, como informação genética.

Consequentemente, a recolha de dados biométricos[3] representa um elevado risco e deve ser considerado o último recurso. A recolha desses dados deve ser avaliado para determinar se realmente é absolutamente necessário, ou se uma solução alternativa pode ser usada. O contexto do projeto, assim como a responsabilidade e capacidade da organização para proteger esses dados cuidadosamente, devem ser considerados. Mesmo que os dados biométricos pareçam a melhor forma de comprovar a identidade das pessoas e evitar a fraude, os riscos potenciais para os beneficiários devem ser avaliados. Especialmente se for provável que outras partes interessadas possam reclamar

[3] Para mais informação, ver o capítulo sobre Dados Biométricos do Manual sobre Proteção de dados, assim como a política sobre dados biométricos do CICV.

esses dados para os seus próprios fins, esse risco poderia ultrapassar as vantagens práticas dos dados biométricos. Além disso, na recolha de dados biométricos, as considerações sobre a sua conservação segura são até mais importantes (ver Capítulo da Orientação Geral).

Além disso, deve lembrar-se o direito de receber informação (transparência). Essas informações devem ser apresentadas de uma forma em que possam ser compreendidas pelas pessoas. O conhecimento e/ou a consciência gerais dos dados biométricos podem ser insuficientes para permitir que as pessoas possam compreender os riscos associados a este tratamento (deve-se salientar que as alternativas ao registo de dados biométricos sempre devem ser consideradas, ver Decisão do Projeto 3 abaixo).

Exemplo:

Várias áreas geográficas foram afetadas por uma pandemia que resultou numa perda de sustentos de vida. Uma intervenção monetária foi decidida para uma comunidade urbana bem desenvolvida e para uma comunidade rural remota. Para o registo, solicitou-se aos chefes das famílias afetadas no contexto urbano que apresentaram uma forma de identificação de uma lista de formulários e documentos válidos para demostrar a sua identidade. Para a comunidade rural, solicitou-se aos chefes das famílias que apresentaram uma certidão do líder/chefe da vila, pois carecem de identificações oficiais. Entregou-se então aos beneficiários da área rural um cartão de identificação temporário expedido pela Sociedade Nacional para exibirem ao fornecedor de serviços financeiros quando reclamarem o dinheiro. Nos dois casos, a recolha de dados biométricos para a identificação foi evitada, e outros meios de deteção da fraude e duplicação foram usados, tais como a comprovação dos nomes e das idades dos membros da família e a expedição de um cupão de um só uso com um código de barras único que foi digitalizado após receberem o dinheiro para indicar que já receberam a sua subvenção.

Decisão do Projeto 2: Que outros dados devo recolher dos beneficiários durante o registo?

🔔 Minimização de Dados, Necessidade

Decisão do Projeto reformulada: Que outros dados dos beneficiários são essenciais para o programa?

Além de recolher os dados para estabelecer a identificação, há outros tipos de dados recolhidos durante o registo para outros fins mencionados acima. Para esses efeitos, é importante considerar quais dados são absolutamente necessários. Tente fazer-se a seguinte pergunta: Para que preciso usar essa informação e é isso essencial para o meu programa? Se não tiver certeza ou se pensar que pode cumprir essa finalidade com outros dados ou de outras formas, deve considerar a opção de não recolher esses dados. Às vezes existe uma tendência a recolher mais dados dos necessários porque pensamos que podem ser úteis posteriormente ou porque essa informação sempre é recolhida, ou porque precisamos dela na nossa base de dados. A criação da base de dados não é um motivo justificado para recolher informações. Pelo contrário, cada elemento dos dados pessoais nessa base de dados deve estar ali por uma razão específica, para alguma coisa bem definida e essencial para o programa.

Uso de modelos padronizados

O uso de modelos padronizados é muito comum e útil no registo, pois acelera a recolha de dados, já que tipos de dados comumente usados foram identificados. No entanto, esses modelos tendem a

abranger uma vasta gama de dados porque pretendem ser um questionário único válido para todos os casos. Porém, numa emergência, esses modelos podem ser usados tal como se encontram, em vez de serem analisados para determinar quais dados são relevantes e essenciais no atual programa que está a ser implementado. A recolha de respostas a essas perguntas irrelevantes entraria em conflito com o princípio de minimização dos dados e de necessidade. Isso não significa que esses modelos não devem ser usados, mas sim que os modelos devem ser analisados e adaptados para cada intervenção. A adaptação não quer dizer voltar a criar novos formulários a cada vez, mas que o mesmo modelo pode ser usado, porém as perguntas que não sejam necessárias devem ser eludidas (ou seja, não ser realizadas se as perguntas se fazem oralmente). Nos arquivos Excel, certas colunas ou filas podem ser ocultadas; no modelo de papel, algumas secções podem ser apagadas ou eliminadas; e no formato digital, os campos podem ser marcados como não necessários[4] ou ocultados. Os membros da equipa que fazem a recolha de dados devem ser informados do princípio de minimização de dados, para eles entenderem por que certas perguntas devem ser eludidas de forma voluntária.

Exemplos:

Num programa monetário visando "famílias que perderam o seu sustento". No dia do registo, pede-se para os beneficiários preencherem o modelo padronizado expedido pela Sociedade Nacional. A equipa tinha analisado o modelo com antecedência e decidiu que as famílias deviam responder todas as perguntas do modelo relativas à sua situação económica. No entanto, a equipa eliminou as perguntas relativas ao estado de saúde dos membros da família. Essa informação não será fornecida, porque nesse programa as famílias recebem a mesma assistência monetária, estejam sãs ou doentes.

A Sociedade Nacional está a responder a uma emergência de seca. Também tem um importante programa de doação de sangue. A equipa está a usar um modelo padronizado que inclui perguntas relativas ao tipo de sangue dos beneficiários. Já que essa informação não é diretamente relevante para a resposta à emergência da seca que estão a elaborar, decidiram não solicitar essa informação aos beneficiários, e os voluntários que estão a fazer a recolha de dados foram informados do motivo. De forma alternativa, poderia ser explicado que os beneficiários podem fornecer opcionalmente a informação sobre o seu tipo de sangue se desejarem participar na campanha de doação de sangue, mas que essa participação não afetaria à assistência proporcionada.

O seguinte mostra diferentes finalidades para a recolha de dados e as considerações essenciais de proteção de dados:

[4] Note-se a distinção entre os dados marcados como "não necessários", que não devem ser perguntados no caso em que a pergunta deva ser respondida para continuar num questionário digital, e os dados marcados como "opcionais", onde a pergunta é feita e é o entrevistado quem se decide responder ou não. As perguntas opcionais devem ser reconsideradas de um ponto de vista de proteção de dados. Em primeiro lugar, as informações não necessárias não devem ser recolhidas. Mesmo que os dados sejam recolhidos de forma voluntária, o princípio da minimização de dados é aplicável. Em segundo lugar, as perguntas opcionais inibem as pessoas a fornecerem informação, e isso pode criar a impressão de que têm mais oportunidades de obter assistência se fornecerem mais informações. Por último, quando a informação seja proporcionada mesmo que não seja diretamente necessária para o projeto, deve-se considerar se existe uma base legítima para tratar esses dados. Deve lembrar-se também que deve ser explicado claramente aos beneficiários quando está a ser solicitada informação "opcional" e deve ficar claro que o fornecimento dessa informação não afetará à assistência proporcionada.

Verificação formal da elegibilidade

Embora somente beneficiários elegíveis sejam invitados a se registar, é possível que a verificação realizada durante o processo de direcionamento não fosse suficientemente formal ou que a situação tiver mudado, e que seja necessário verificar de novo a elegibilidade durante o processo de registo. Aqui, deverão ser recolhidos dados relativos aos critérios acordados de direcionamento. As considerações relativas a isto foram discutidas anteriormente no capítulo sobre Direcionamento. Essas considerações são aplicáveis durante o processo de registo, em particular a pergunta de se certas informações teriam um impacto sobre a decisão de visar uma pessoa. Se esse for o caso, essa informação pode ser recolhida. Caso contrário, não existe motivo para fazê-lo.

Nas distribuições globais nas quais não existem critérios específicos de direcionamento porque todas as pessoas da área precisam de assistência, a recolha de dados de elegibilidade pode não ser necessária, a menos que sejam requeridos para saber que as pessoas são da área afetada ou estabelecer a autenticação para receber assistência. O processo de registo neste caso, não requer perguntar sobre os indicadores de vulnerabilidade, nem outras questões tipicamente usadas para estabelecer a elegibilidade. Também pode não ser necessário fazer perguntas para recolher dados demográficos usuais (tais como idade, género ou dimensão da família), a menos que tenham uma finalidade relevante, pois esses dados não são usados para visar os beneficiários.

Realização da distribuição monetária

Quais dados são requeridos para permitir a distribuição monetários aos beneficiários depende do método de distribuição escolhido. Para a entrega de dinheiro em envelopes, os principais dados para recolher podem estar limitados à informação de identidade básica e de autenticação para ser usada durante a distribuição. Quando fornecedores de serviços financeiros (FSF) forem usados, mais dados podem ser necessários, incluindo os dados *Know Your Customer* (KYC) requeridos por lei para os FSFs distribuírem o dinheiro. Detalhes sobre a recolha de dados para o seu uso pelos FSFs serão discutidos de forma mais pormenorizada no seguinte capítulo. Durante o registo, é importante considerar de forma crítica o que é necessário e requerido para permitir a distribuição monetária (por exemplo, números móveis para receber o dinheiro móvel).

Evitação da fraude e da duplicação

A fim de evitar a fraude e a duplicação de pagamentos, pode ser necessário recolher informações adicionais para triangular a informação básica do agregado familiar: por exemplo, recolher os nomes, idades e género de todos os membros da família e realizar uma comprovação de se qualquer um deles tiver tentado se registar como um agregado familiar separado. Também, para os programas que dependem do tamanho do agregado familiar para determinar a quantia monetário a desembolsar, pode ser necessária a comprovação detalhada dos agregados familiares (por exemplo, através de cartões familiares expedidos pelo governo). Nesses casos, é importante refletir no contexto real para avaliar o risco, e depois assegurar-se de que a recolha e o tratamento de dados são apropriados para o nível de risco avaliado, em vez de recolher esses dados de uma maneira padronizada.

Exemplos:

O programa monetário foi estabelecido para responder a um calor extremo que causou incêndios numa pequena vila. O critério-alvo (famílias que perderam a casa) abrange quase todas as famílias da vila. Os nomes dos chefes dessas famílias são indicados e confirmados pelos líderes comunitários. No dia de registo, pede-se para os chefes das famílias se identificarem. A equipa decide que não vai recolher dados relativos aos membros da família. O risco de fraude não é muito elevado, pois a maioria de famílias vão receber assistência e os chefes das famílias foram claramente identificados e registados em colaboração com a comunidade. Consequentemente, é improvável que outros membros das famílias ou pessoas de outras vilas possam reclamar assistência de forma fraudulenta.

Um programa monetário foi estabelecido para responder uma situação de insegurança alimentar numa pequena comunidade, visando famílias chefiadas por mulheres. A subvenção monetária é relativa ao tamanho da família para satisfazer as suas necessidades. A equipa do programa decide que vai recolher o número do agregado familiar, pois é necessário para o cálculo da subvenção, mas que provavelmente não seja necessário recolher informação adicional sobre os membros individuais da família. Sendo uma comunidade pequena, é improvável que as pessoas tentem indicar números maiores para o tamanho do agregado familiar, pois outros membros da comunidade provavelmente conhecem esse dado e podem informar da discrepância.

O mesmo programa monetário foi implantado nas comunidades maiores e mais dispersas. As subvenções monetárias são maiores devido aos ajustes do custo da vida. Houve informações de aumento artificial do tamanho dos agregados familiares em anteriores programas geridos por outras ONGs. A análise da equipa do programa indicou um risco elevado de fraude potencial e decidiu recolher informações adicionais sobre os membros das famílias (nome, idade, género, grau de filiação). Dados adicionais foram usados para comprovar duplicados na lista de beneficiários registados.

Nota: Para os programas que usam autodirecionamento ou autoregisto, onde os beneficiários se candidatam de acordo com critérios de direcionamento publicados, é importante indicar que também são recolhidos dados para aqueles que não cumprem a elegibilidade. Recomenda-se assegurar que, quando seja óbvio que a pessoa não é elegível, os seus dados sejam eliminados ou arquivados para impedir novas tentativas de registo (conforme necessário). Se for necessária uma verificação complementar, os dados deverão ser conservados por um tempo limitado até que o processo de verificação seja realizado e, se o solicitante não for elegível, deverá ser informado e os seus dados deverão ser eliminados em conformidade. Ver o capítulo de Considerações gerais no tocante à conservação de dados das pessoas não beneficiárias. Além disso, é importante assegurar-se que os critérios de direcionamento publicados sejam reduzidos e detalhados, a fim de limitar o número de solicitantes não elegíveis.

Decisão do Projeto 3: O que devo dizer aos beneficiários sobre o tratamento dos seus dados?

Transparência

Decisão do Projeto reformulada: Como posso garantir que os beneficiários tenham acesso à informação relativa ao tratamento dos seus dados?

O princípio de proteção de dados da Transparência significa que os beneficiários, como pessoas em

causa, devem receber uma comunicação clara sobre o motivo pelo qual os dados deles são recolhidos e como esses dados estão a ser tratados. Isto inclui a finalidade da recolha, a conservação, a potencial partilha de dados, os direitos dos beneficiários, etc. Informar ao beneficiário sobre todo isto pode ser desafiante nalgumas situações, em particular nas emergências onde o tempo está limitado. Além disso, quando os beneficiários têm necessidades mais urgentes do que a proteção de dados, podem não ter tanto interesse em conhecer esses detalhes ou em entender o seu significado. Contudo, têm direito a receber essa informação.

Uma boa abordagem é proporcionar aos beneficiários alguma **informação básica** e um **contacto** ao qual acudir se quiserem saber mais. Isto deve ser incluído no plano de Engajamento Comunitário e Responsabilização do programa (ver Módulo M4_2 do *kit* de ferramentas de AMeE). A informação básica pode ser fornecida durante a reunião com as comunidades para explicar o programa e pode ser repetida durante o processo de registo de beneficiários. A Sociedade Nacional também pode preparar, imprimir e compartilhar um aviso geral de privacidade, junto com os detalhes do programa (ver modelo do Aviso de Privacidade na seção de referências). Os beneficiários podem consultar esse aviso e, se for necessário, entrar em contato com a Sociedade Nacional para obter mais informações quando precisarem. O elemento fundamental é que os beneficiários possam entrar em contacto com alguém através de uma linha de atendimento telefónico ou presencial.

Ao fornecer informações sobre o tratamento de dados, é importante a empatia e perguntar-se: Quais as informações preciso saber antes de fornecer os meus dados pessoais? As informações básicas comuns são indicadas abaixo. Essas informações devem ser apresentadas claramente, de uma maneira simples de compreender e na língua ou línguas apropriadas.

- **Finalidade da recolha de dados no dia de registo.** Consultar as finalidades estabelecidas para o seu programa algumas finalidades comuns discutidas anteriormente incluem a necessidade de provar a identidade, a comprovação da elegibilidade, a realização da distribuição monetária ou a evitação da fraude e da duplicação. Os beneficiários precisam saber esses motivos e o motivo pelo qual alguns dados são necessários para esses fins; isso ajuda-lhes a compreender o que está a acontecer.
- **Se foram recolhidos dados sobre eles de outros** (por exemplo, outras ONGs, líderes comunitários, governo). Frequentemente recebem-se informações dos beneficiários de outras fontes antes de entrar em contato com eles diretamente. É importante para os beneficiários saberem onde foi obtida a informação pessoal deles, para que possam ter confiança em que os seus dados estão a ser usados com responsabilidade.
- **Como corrigir dados inexatos.** Para os beneficiários é tranquilizador saber que podem corrigir dados imprecisos em qualquer momento. Ocorrem erros, em especial quando as ações se realizam de forma precipitada numa emergência, tanto por parte da equipa do programa que faz a recolha de dados quanto pelo beneficiário que fornece os dados iniciais. Se for descoberto que a informação é incorreta, o beneficiário deve poder solicitar a correção.
- **Como expressar preocupações ou apresentar queixas.** Os beneficiários devem saber que podem expressar as suas preocupações sobre o tratamento dos seus dados. É importante que eles saibam isso, pois lhes dá um senso de controlo. Podem querer opor ao tratamento de dados ou reclamar sobre ele. Se for o caso, devem saber aonde ir e com quem podem falar sobre suas preocupações e opções. Isso deve ser parte do *feedback* e do mecanismo de reclamação do programa (ver Módulo M4_2_5 do *kit* de ferramentas de AMeE).
- **Intenção de compartilhar dados.** Se souber que vai compartilhar os dados recolhidos com outros grupos ou instituições (tais como outras ONGs, FSFs, governo), o beneficiário deve saber disso e o motivo pelo qual é necessário compartilhar os dados. Afinal, o beneficiário fornece essa informação consigo e confia em que irá manter a segurança da mesma.

Nalguns contextos, o beneficiário pode não querer que alguns tipos de informação sejam compartilhados com outras entidades devido a motivos de sensibilidade ou segurança. Pode ser útil a realização de uma *due diligence* sobre essas instituições, para poder comunicar a sua fiabilidade em termos do tratamento de dados de beneficiários. Além disso, se os beneficiários detetarem um potencial uso indevido de suas informações porque foram compartilhadas com entidades externas, devem ser animados a informar à Sociedade Nacional através do serviço de assistência ou por meio de contacto direto para essas questões.

Além da informação básica mencionada acima, seria bom preparar detalhes adicionais sobre o tratamento de dados para possíveis novas perguntas dos beneficiários. As outras informações que os beneficiários devem receber (em função do contexto) incluem:

- Conservação dos dados e medidas de segurança;
- Período de conservação previsto para os dados;
- Base legítima para o tratamento;
- Quaisquer informações adicionais sobre a finalidade ou o tratamento posterior;
- Quaisquer informações adicionais sobre partilha de dados;
- Outros direitos da pessoa em causa que possam ser aplicáveis, como o direito de apagamento, de objeção e de acesso aos dados;

Decisão do Projeto 4: Devo solicitar aos beneficiários o seu consentimento?

Base Legítima

Decisão do Projeto reformulada: Em que base legítima devo basear-me?

A questão de saber se se deve pedir ao beneficiário seu consentimento relativo à recolha e o uso de seus dados tem muitas capas. Virou prática comum iniciar os formulários de registo dos beneficiários com uma pergunta sobre o consentimento antes de proceder. À primeira vista, parece correto fazer isso, obter permissão é educado e respeitoso. No entanto, de acordo com a lei de proteção de dados, o tratamento de dados pessoais pode basear-se noutros motivos além de somente o consentimento, o que se discutirá com mais detalhe abaixo.

Ainda assim, não seria melhor pedir o consentimento? Não necessariamente. Pode parecer um sinal de respeito pedir ao beneficiário o seu consentimento, mas isso traz consigo alguns desafios que devem ser considerados.

Problemas com o consentimento

O consentimento deve ser outorgado livremente e com pleno conhecimento. Na prática, isso quer dizer que o consentimento só é válido quando existir uma opção real de recusá-lo; no caso contrário, não é "outorgado livremente". Em caso de emergências, a obtenção do consentimento pode não ser factível. Os beneficiários estão numa situação vulnerável e desesperada, na necessidade de ajuda imediata. A proteção de dados pode não ser a primeira preocupação deles. Assim, é possível que forneçam o seu "consentimento"[5] porque não vêm outra opção para obter ajuda. E efetivamente, sem os dados deles é impossível ajudá-los.

Além disso, os beneficiários podem não estar em situação de compreender plenamente as consequências de fornecerem os seus dados ou como os dados são tratados (por exemplo, por meios

[5] O consentimento está escrito entre aspas porque, embora o beneficiário possa marcar um quadrado ou fazer outra indicação de que outorga o seu consentimento, não seria correto dizer que seria legalmente reconhecido como consentimento de acordo com as leis e os princípios gerais de proteção de dados.

tecnológicos). Não é possível aceitar de forma significativa o que não se compreende (e, portanto, não pode ser considerado um "conhecimento pleno").

Uma outra questão para considerar é que o consentimento pode ser retirado a qualquer momento (se foi outorgado livremente, pode ser livremente retirado). Uma vez que o consentimento for revocado, qualquer tratamento posterior dos dados pessoais em causa (realizado de acordo com esse consentimento) é proibido. Isto pode tornar-se muito problemático para o programa, pois é importante contar com um conjunto de dados confiável para trabalhar. Uma vez que o consentimento for retirado, pode não ser mais possível voltar para atrás e usar outra base legítima, tal como o interesse vital ou o interesse público. Por quê? Porque o direito de retirada não tem valor se não muda nada posteriormente, e também depende de se outra base legítima pode ser identificada e que informações já foram fornecidas ao beneficiário. Por todos esses motivos, usar o consentimento como base legítima pode ser problemático. Para o tratamento de dados pessoais no contexto dos programas monetários em emergências, recomenda-se considerar outras opções.

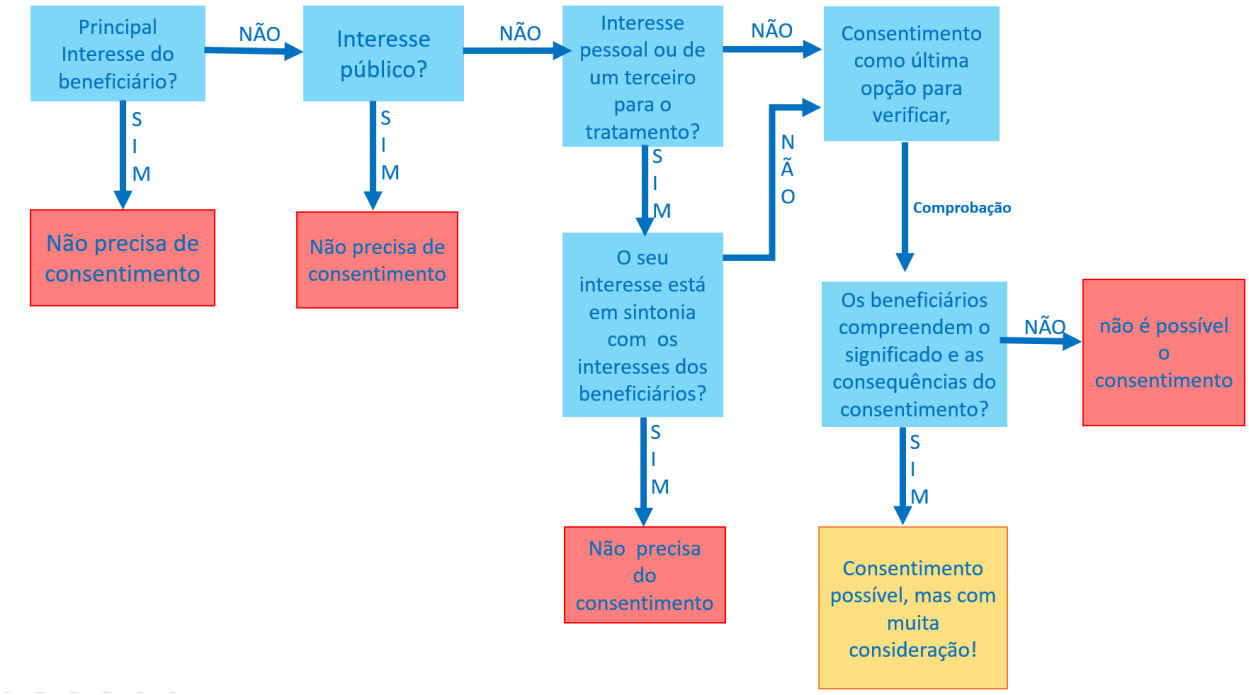

Figura 3: Árvore de decisão para determinar se o consentimento é uma base legítima apropriada

Outras opções

A Figura 3 mostra outras opções para o estabelecimento da base legítima. Duas dessas opções são o interesse vital e o interesse público. O **interesse vital** significa que o tratamento dos dados pessoais é essencial para a vida, integridade, saúde, dignidade ou segurança dos beneficiários. Os programas de AMV desenhados para abordar necessidades vitais ou essenciais no início de uma emergência podem beneficiar-se disto; para outras atividades de AMV num contexto de não emergência, pode ser necessário investigar outras opções. O **interesse público** significa que o tratamento de dados pessoais serve uma finalidade que é do interesse de todo o mundo. As Sociedades Nacionais que fornecem assistência cumprem um mandato humanitário que é do interesse público geral. Assim, embora o alto padrão do interesse vital não seja cumprido, normalmente a assistência através de AMV ainda será no interesse público[6].

[6] Note-se que nalgumas jurisdições, basear-se no interesse público pode requerer considerações adicionais ou uma autorização governamental oficial. Vai além do âmbito desta orientação verificar isto para cada jurisdição. Se tiver dúvidas sobre se é possível se basear no interesse público para o seu programa, não duvide em comunicar com o seu diretor ou a equipa legal da Sociedade Nacional.

Para evitar equívocos: é opção dos beneficiários se desejarem participar no programa ou não. Mas se decidirem fazê-lo, é aceitável usar os dados pessoais deles sem pedir o consentimento explicitamente sempre que tiverem sido informados sobre o programa e sobre o uso desses dados. É no interesse vital deles e/ou no interesse público. O importante é usar somente os dados pessoais que sejam absolutamente necessários para o programa. Ver também a seção sobre a Programação de Transferência Monetária do Manual sobre Proteção de Dados para mais detalhes sobre as bases legais para a AMV.

Partilha de dados

A partilha de dados com outras entidades (tais como outras ONGs, governo, FSFs) pode ser no interesse vital dos beneficiários ou no interesse público. Além disso, pode haver obrigações legais de compartilhar alguns dados pessoais[7] e, nesse caso, pode ser feito sem consentimento. Quando não houver obrigação legal, pode ser no interesse legítimo da Sociedade Nacional compartilhar dados pessoais. O interesse legítimo pode justificar a partilha de dados sem consentimento se os beneficiários não tiverem um interesse oposto e dominante. É crucial considerar as consequências ou riscos potenciais da partilha dos dados para os beneficiários. Isto explica-se com mais detalhe no Capítulo sobre Partilha de Dados. Em suma, tudo se resume à necessidade e à confidencialidade.

Administração do programa

Algumas decisões do projeto relativas ao tratamento dos dados podem não ser diretamente no interesse vital ou público, mas ainda são razoáveis na perspetiva do programa (por exemplo, tipo de armazenagem, inclusão de mais membros da equipa, etc.). De novo, entra em jogo o interesse legítimo da Sociedade Nacional para estruturar e organizar o programa de forma efetiva e eficiente.

Então?

Na maioria dos casos, não é necessário recolher o consentimento. Isso não quer dizer que as ações estejam menos justificadas, pelo contrário. Contudo, há mais pontos a considerar:

- Não pedir o consentimento não quer dizer que não seja necessário **informar os beneficiários**! Independentemente da base legítima que quiser usar, o princípio da Transparência é aplicável. Como se descreve na Decisão do Projeto 3, o fornecimento de informação básica sobre o tratamento dos dados pessoais e de um contacto para perguntas complementares são boas práticas.
- Pode considerar a substituição da pergunta sobre o consentimento por “antes de proceder, tem alguma pergunta ou preocupação?” ou “reconhece ter recebido informação básica sobre o programa, incluindo onde pedir mais detalhes sobre qual será o uso dos seus dados?” Isto não é obrigatório, mas pode ser uma forma alternativa de ser educado e respeitoso antes de solicitar mais dados pessoais.
- É preciso avaliar a base legítima para cada intervenção de AMV que fizer? Não necessariamente. A maioria das intervenções de AMV pode abranger a mesma base legítima. Só lembre-se de não usar o Consentimento como base por defeito. Se a categoria de um novo programa de AMV é única e os impactos sobre os dados dos beneficiários não são claros, seria bom avaliar formalmente a base legítima antes de proceder. Também é aconselhável realizar uma Avaliação de Impacto na Proteção de Dados nesse caso. Ver Capítulo da Orientação Geral para mais detalhes sobre isto.

V. Uso de Fornecedores de Serviços Financeiros

Uso de Dados Pessoais

A distribuição de assistência monetária e através de vouchers é feita geralmente com o apoio de fornecedores de serviços e, portanto, um contrato é estabelecido com eles. No caso dos programas que incluem vouchers, os fornecedores incluem empresas de negociações de mercadorias, fornecedores locais, supermercados e grossistas. Para os programas monetários, são fornecedores de serviços financeiros (FSF), tais como bancos, operadores de redes móveis ou agentes de remessas que realizam entregas de dinheiro. Para este capítulo, focalizaremos nos FSFs, mas note-se que os princípios de proteção de dados devem ser considerados para todos os tipos de fornecedores de serviços. O uso de fornecedores de serviços pode ser revisto no Módulo M4_3 do *kit* de ferramentas de AMeE.

Considerações de Proteção de Dados

O uso de FSFs pode requerer a partilha de dados pessoais de beneficiários para poder distribuir dinheiro. Esta secção examinará as decisões do projeto essenciais no trabalho com os FSFs e as considerações ligadas à proteção de dados. Os riscos relativos à proteção de dados e aos FSFs devem ser incluídos na Matriz de Riscos de AMV do programa desenvolvida de acordo com as fases de Avaliação e Análise da Resposta do programa. Ver Módulo M2_4_3 Avaliação e Módulo M3_1_4 Análise da Resposta do *kit* de ferramentas de AMeE.

Decisão do Projeto 1: Devo usar um Fornecedor de Serviços Financeiros?

Minimização de Dados, Necessidade e Segurança dos Dados

Decisão do Projeto reformulada: Pode o FSF usar dados dos beneficiários de uma forma que seja prejudicial para os beneficiários?

Ao considerar se usar um FSF no projeto, é importante analisar quais dados serão requeridos pelo FSF para fornecer o serviço, o que pode envolver pedir informações adicionais aos beneficiários com esse fim, e avaliar cuidadosamente as potenciais consequências para os beneficiários da partilha desses dados.[8]

Know Your Customer* (KYC) e *Watch List Screening

Muitos FSFs estão sujeitos à regulação KYC, que lhes exige recolher informação sobre os clientes para impedir a lavagem de dinheiro, o financiamento do terrorismo ou outros crimes. A quantidade de informação necessária poderia depender das regulações locais com alguns países que permitem maior flexibilidade em função do nível de risco das transações. As agências humanitárias que usam FSFs deverão cumprir com essas regulações KYC que exigem a partilha de alguns dados dos beneficiários.

Algumas considerações para assegurar que o princípio de minimização e necessidade é cumprido:

- Investigar as regulações KYC no seu país e no seu contexto operacional. É preciso determinar quais dados são requeridos por lei e cotejar isso em relação ao que o FSF solicita. Pode haver políticas internas para explicar por que os FSFs estão a solicitar dados adicionais fora do que é exigido por lei; isto deve ser justificado e negociado para garantir que somente seja compartilhado o estritamente necessário para prestar a assistência.
- Nalguns casos, as organizações humanitárias podem advogar por requisitos KYC simplificados ou ajustados (por exemplo reduzindo os requisitos para as pessoas que perderam as suas identificações, estabelecendo as quantidades máximas que podem ser transferidas aos beneficiários ou terceiros em relação ao KYC, ou permitindo transferências monetárias durante um tempo limitado). Comprovar se nesses casos os

dados compartilhados com os FSFs podem ser minimizados.

- Informar aos beneficiários e explicar os requisitos de KYC ou como mínimo incluir esses requisitos no aviso de privacidade, que pode ser consultado a qualquer momento.

Os FSFs podem ter obrigação de comprovar a informação de KYC e compartilhar dados com terceiros (tais como reguladores e autoridades públicas). Essas comprovações de KYC podem incluir cotejar a lista dos beneficiários com listas de vigilância, listas de sanções ou listas de pessoas designadas pelas autoridades locais que possam estar envolvidas em conflitos ou violência. Alguns FSFs fazem isso de forma sistemática, e outros a pedido do governo. Este processo assinalará pessoas que possam ser suspeitas de estarem envolvidas em certas atividades criminais (lavagem de dinheiro, terrorismo, corrupção, etc.) e, portanto, não elegíveis para receber dinheiro. Se o nome de um beneficiário estiver incluído numa dessas listas, isto pode ter graves consequências para eles. Portanto, é essencial analisar o contexto do país e do programa. As seguintes são perguntas habituais a considerar:

- Existem denúncias de perseguição política, étnica ou religiosa pelo governo?
- Há partes da população de beneficiários que são consideradas oponentes do regime?
- Podem os partidos políticos ser considerados grupos terroristas?
- Está o FSF estreitamente ligado com as autoridades estaduais, como serviços de inteligência ou agências de segurança?
- Se os beneficiários forem refugiados, tem o FSF uma sucursal ou uma instalação de armazenagem no país de origem dos refugiados na qual as autoridades possam solicitar os dados?
- Teriam os beneficiários graves preocupações ou medo se os seus dados forem compartilhados de algum modo com o governo devido a essas obrigações?

Se suspeitar que os dados dos beneficiários podem ser usados de forma inapropriada, isto apresenta um grave risco para os beneficiários. Nestas circunstâncias, se não for possível encontrar uma forma para contratar com um FSF sem compartilhar dados de beneficiários, outras opções de distribuição devem ser consideradas, como dinheiro em envelopes, vouchers, ou inclusive em espécie. Isto deve ser feito como parte da Avaliação de riscos na fase de Resposta e Análise do programa (Módulo 3 do *kit* de ferramentas de AMeE) e deve incluir uma análise de se a perseguição, a exclusão ou outras sensibilidades poderiam resultar na recolha e partilha de informação de KYC na seleção da modalidade de melhor transferência. Outras referências de CaLP: Normas de *Know Your Customer* e Recomendações de Privacidade para a Transferência Monetária e Folha de Dicas das Regulações de KYC.

Outras finalidades

Sendo que geralmente os FSFs são empresas com fins lucrativos, poderiam usar os dados dos beneficiários para os seus fins, incluindo interesses comerciais, tais como a realização de perfis em relação à situação de solvência, publicidade ou marketing, e a comprovação de elegibilidade para outros serviços financeiros. Esses exemplos podem parecer relativamente de risco baixo para os beneficiários, mas ainda são considerados fora da finalidade da assistência monetária humanitária. A lei de proteção de dados também pretende proteger as pessoas das ações não solicitadas de instituições privadas, como o envio de spam.

Outro impacto potencialmente elevado da reutilização de dados pelos FSFs poderia ser para a compensação de dívidas (por exemplo, o beneficiário deve um préstamo ou dinheiro ao banco e o banco trata de deduzir a assistência monetária para compensar o devido) ou a nova partilha de dados com terceiros, tais como cobradores de dívidas.

Em geral, deve fazer-se uma *due diligence* sobre a reputação e o rendimento dos FSFs durante o processo de concurso ou contratação.[9] Além disso, os contratos com os FSFs devem restringir o tratamento complementar de dados (durante a distribuição monetária e inclusive depois dela), e incluir exemplos de ações que devam ser evitadas, se forem conhecidas no momento da contratação (ver Decisão do Projeto 3). Durante a implementação do programa, deve-se pedir/solicitar para os beneficiários comunicarem à Sociedade Nacional qualquer caso de uso complementar (ou uso indevido suspeito) dos seus dados por parte de FSFs que estejam fora do programa.

Decisão do Projeto 2: Que tipo de conta devo escolher para a distribuição monetária?

Minimização de Dados, Necessidade e Segurança dos Dados

Decisão do Projeto reformulado: Que tipo de conta usar para a distribuição monetária protegendo melhor os dados dos beneficiários?

Existem diferentes mecanismos de pagamento em dinheiro a considerar, incluindo o uso de bancos, agências de remessas, fornecedores de redes móveis e agências de correios. Numa perspetiva de proteção de dados, independentemente de qual for a opção do mecanismo de pagamento selecionada, é importante considerar como limitar a partilha de dados pessoais. Isso pode depender basicamente do tipo de conta usado para a distribuição monetária. Deve-se considerar o uso de dois tipos de contas: o uso de contas nomeadas para beneficiários individuais ou de uma conta virtual gerida pela Sociedade Nacional.

Contas nomeadas

O programa pode optar por usar diretamente a conta do beneficiário com o fornecedor de serviços financeiros ou abrir uma conta pessoal. O uso de contas preexistentes de beneficiários interfere menos com a proteção de dados do que abrir contas novas, pois o FSF e o beneficiário já têm uma relação contratual que a Sociedade Nacional aproveita para efeitos do programa. A criação de novas contas para beneficiários individuais pela Sociedade Nacional, supondo que for viável, deve ser analisada com mais detalhes para determinar os possíveis riscos de proteção de dados. Por exemplo, pode haver uma razão específica pela qual o beneficiário não abriu a sua conta individual (como por exemplo, algumas preocupações relativas ao KYC mencionadas na seção acima). Abrir uma conta em nome de outra pessoa requer atenção na recolha e partilha de dados com o FSF, assim como a gestão dessa conta depois do programa.

Contas virtuais

As contas virtuais são propriedade da organização humanitária e geridas por ela, nas quais subcontas podem ser criadas para os beneficiários poderem receber dinheiro. Com essas contas, o KYC se faz com a organização e não com os beneficiários individuais. Exemplos de uso de contas virtuais:

- Expedição de cartões multibanco pré-pago, senda cada cartão ligado à conta da Sociedade Nacional e fornecido a pessoas elegíveis com um código PIN que pode ser usado para o levantamento do dinheiro;
- Expedição de cheques bancários a pessoas, que podem ser cobrados independentemente de ter uma conta nesse banco;
- Cartão SIM móvel de uso limitado expedido pela organização, a fim de que os beneficiários possam receber um SMS com códigos transacionais que podem ser usados para levantamento do dinheiro nos agentes de dinheiro móvel

[9] Pode-se encontrar um modelo de questionário para FSFs na seção de referências desta orientação.

Ainda assim, os dados dos beneficiários podem dever ser compartilhados a efeitos de identificação no momento do desembolso monetário, mas a quantidade de dados que deve ser compartilhada com o FSF é geralmente reduzida em comparação com a criação de contas nomeadas, pois não se estabelece o KYC com as pessoas. Numa perspetiva de proteção de dados, esta opção é atrativa, mas também há algumas considerações operacionais (tais como a capacidade da equipa do programa para gerir as subcontas, a distribuição de elementos como os cartões pré-pago para receber dinheiro às pessoas corretas e ligados aos números de subconta corretos, e a reconciliação das transações após o desembolso). O risco de gestão das transações e dos fundos corresponde maioritariamente à agência. Também, no uso de contas virtuais, a SN tem acesso a dados que revelam como os beneficiários usam o dinheiro. Esses dados são sensíveis. A fim de respeitar a privacidade dos beneficiários neste sentido, consulte o capítulo sobre Monitoramento Após a Distribuição para mais detalhes sobre a privacidade e o monitoramento.

Decisão do Projeto 3: O que deve incluir o contrato com o FSF?

Segurança dos Dados

Decisão do Projeto reformulado: Que disposições devo incluir num contrato com o FSF para proteger os dados pessoais dos beneficiários?

Em primeiro lugar, é importante determinar quais são os dados absolutamente necessários para fornecer o serviço do FSF e negociar para minimizar a partilha de dados. Isto incluiria geralmente:

- Dados de identificação, como o nome do beneficiário e um número de ID válido;
- Dados requeridos de KYC, que podem variar em função das regulações nacionais;
- E outros dados, quando aplicável, requeridos para permitirem a distribuição monetária, tais como: número de telefone móvel para transferências de dinheiro móvel, número de conta bancária, ou nome e identificação da pessoa autorizada a receber o dinheiro em nome do beneficiário (representante);

Também é importante compreender quais dados podem ser criados pelo FSF e compartilhados consigo como parte das transações realizadas com os beneficiários. Por exemplo, a data e a situação do pagamento, a assinatura do beneficiário após receber o dinheiro, o saldo atual se todo o dinheiro não tiver sido retirado ainda, onde o dinheiro pode ter sido usado (por exemplo, mercado), etc.

Em segundo lugar, um contrato ou acordo de serviços deverá ser estabelecido. Esse contrato deverá incluir o quadro para a prestação de serviços, o âmbito e os elementos de proteção de dados. Recomenda-se contar com um modelo para esse contrato elaborado e compartilhado como parte do processo de concurso, e as considerações de proteção de dados avaliadas como parte da seleção do fornecedor.

Algumas das disposições essenciais que devem ser incluídas no contrato são as seguintes:

- **Limitação das finalidades.** Os dados compartilhados só serão usados para os efeitos do programa (distribuição monetária). Não será permitido nenhum outro uso fora do âmbito do programa. Tal como foi mencionado acima, também pode ser útil ser explícito ou enumerar concretamente os exemplos das finalidades para as quais os dados não devem ser usados (tais como publicidade e marketing, compensação de dívidas). A lista deve ser marcada como “não exaustiva”.
- **Partilha dos dados com outros.** O FSF não compartilhará os dados com outros se isso não for aprovado pela Sociedade Nacional. Também, em caso de obrigação de partilha (por exemplo, com as autoridades), a SN deve ser informada a primeira.

- **Segurança dos dados.** Os dados compartilhados serão conservados de forma segura (por exemplo, indicar controlos de acesso, encriptação, processos de *backup*).
- **Confidencialidade.** Os dados compartilhados serão tratados de forma confidencial.
- **Nenhuma recolha adicional de dados do beneficiário.** O FSF não deve recolher outros dados pessoais do beneficiário ao abrigo do programa: por exemplo, o beneficiário pode ter de mostrar as suas identificações ao reclamar a assistência monetária, mas o FSF não deve fazer uma cópia nem digitalizar a identificação e assim recolher dados adicionais do beneficiário.
- **Eliminação.** Os dados compartilhados serão eliminados das bases de dados do FSF após a execução do programa, ou arquivados fora de linha e de forma segura para efeitos de auditoria.
- **Consequências de uma vulneração por parte do FSF.** O contrato deve conter menções indicando que o FSF reconhece que uma vulneração desses termos pode ter consequências legais, ou como mínimo causar danos à reputação de todas as partes envolvidas. Deve indicar-se que se anima aos beneficiários a informar à Sociedade Nacional de qualquer uso não ligado ao programa dos seus dados pessoais pelo FSF.

Consultar a seção de referência abaixo para ver um exemplo de modelo da FICV para a contratação com os FSFs. Contém os pontos relevantes sobre proteção de dados. Se considerar que falta alguma coisa ou quiser abordar uma questão específica que surgiu no contexto do seu programa, pode adicionar esses aspectos no seu próprio modelo.

Na prática, com frequência o FSF quer usar o seu próprio modelo de contrato. Em função da sua posição negociadora, tente negociar com o modelo preparado pela Sociedade Nacional. Se finalmente o modelo do FSF é usado, é aconselhável analisar mais aprofundadamente, comparar os elementos de proteção de dados e solicitar que sejam alterados para garantir uma elevada proteção dos dados dos beneficiários. Se o modelo do FSF não contiver nenhuma menção sobre proteção de dados, é a sua oportunidade para introduzir os elementos de proteção de dados que considerar importantes. Pode aproveitar algumas cláusulas do modelo da FICV. Se o FSF não quiser aceitar nenhuma menção sobre proteção de dados no contrato, deve ser um sinal de alerta no tocante à colaboração com esse fornecedor. Qualquer entidade reputada deve ter interesse num nível mínimo de proteção de dados.

É comum negociar um acordo-quadro com um ou vários FSFs como parte da preparação monetária, para ter opções em função do contexto e das necessidades. Contudo, novos programas podem gerar novas situações não incluídas no contrato atual com o FSF. Se tiver a impressão de que a proteção de dados não é suficientemente tratada no acordo-quadro, não duvide em comunicá-lo ao FSF ou a seu diretor para tentar negociar uma emenda. A proteção de dados tornou-se cada vez mais importante nos últimos anos e a sensibilização com este assunto apenas começou.

VI. Partilha de Dados com o Governo, outras Organizações Humanitárias e Doadores

Uso de Dados Pessoais

As intervenções de AMV requerem a cooperação e a coordenação com outras partes interessadas, tais como o governo nacional, outras organizações humanitárias (internacionais e nacionais) e doadores. Nessas relações, é possível que os dados dos beneficiários de uma Sociedade Nacional terão de ser compartilhados externamente (e que a Sociedade Nacional também receba dados). A partilha pode ser feita formalmente através de contratos de partilha de dados ou informalmente sem contratos estabelecidos, em particular nas emergências nas quais a prontidão é essencial.

No capítulo sobre Direcionamento, vimos exemplos de receção de dados de beneficiários do governo e de outras organizações em resposta à mesma emergência para estabelecer uma lista preliminar de beneficiários e comprovar a elegibilidade das pessoas incluídas na lista. Este nível de partilha de dados também é importante para a coordenação entre os vários atores a fim de evitar uma custosa duplicação de esforços e da assistência. Para os doadores, pode haver algumas obrigações de auditar e demostrar a transparência e a responsabilização garantindo que os beneficiários que têm recebido a assistência são pessoais reais, eram efetivamente elegíveis e efetivamente receberam a assistência monetária.

Considerações de Proteção de Dados

Neste capítulo, analisaremos as considerações de proteção de dados na partilha de dados com partes externas. Em geral, na partilha de dados com diferentes partes, **é importante garantir que os dados sejam transferidos de forma segura por meios seguros** (por exemplo, arquivos encriptados, conservados nas salas de dados protegidas) e partilhado só com pessoal autorizado. Ver capítulo de Orientação Geral.

Quando os dados forem transferidos a outros países, é essencial avaliar o nível de proteção no país. Se for inferior ao padrão da SN, a transferência deve ser reconsiderada e, se for inevitável, deve negociar-se um contrato de partilha de dados sólido e detalhado relativo aos requisitos de proteção de dados.

Decisão do Projeto 1: Quais dados devo compartilhar com o governo?

🔔 Segurança dos Dados e Necessidade

Decisão do Projeto reformulado: É necessário e seguro compartilhar dados pessoais com o governo?

As Sociedades Nacionais, apesar de atuarem como auxiliares do governo do seu país, têm a obrigação de manter a sua natureza neutral, imparcial e independente no que diz respeito à ação humanitária. Porém, também estão sujeitas as leis nacionais[10] nas quais pode haver obrigações legais e, portanto, vinculativas de compartilhar certos dados com o governo. Alguns dos riscos de proteção de dados foram discutidos na seção sobre KYC (em relação ao uso dos FSFs) em quanto à informação sobre pessoas designadas às autoridades (listas de vigilância, listas de sanções). Também pode existir o risco de que a Sociedade Nacional seja pressionada pelas autoridades para compartilhar dados pessoais para outros efeitos (por exemplo, combater o terrorismo). Portanto, na preparação de intervenção de AMV— muito antes de recolher os dados— é necessário analisar e documentar esses riscos (através de una matriz de riscos ou de uma análise mais estruturada através de uma AIPD).

Além das leis nacionais específicas, existem outras finalidades para as quais os dados podem ser requeridos pelo governo à organização:

- **Obter compreensão da intervenção de AMV.** Com frequência, o governo deseja ser informado dos programas humanitários organizados na sua jurisdição, pois é o responsável último da segurança e o bem-estar dos cidadãos e habitantes da sua área. Além disso, se houver desacordos de alguns membros da comunidade sobre por que não foram incluídos no programa, podem levar as suas queixas às autoridades. Geralmente, as autoridades desejam compreender a finalidade, a duração, os grupos-alvo e os critérios de condução acordados, a escala financeira, os requisitos de segurança, os recursos e o apoio requerido. Para o governo obter uma compreensão do programa, normalmente basta fornecer informação geral e dados agregados (critérios de direcionamento, áreas, número de pessoas apoiadas, percentagem de maiores/crianças, quantidade da subvenção monetária, etc.). Em alguns casos, podem ter interesse em ver a lista final de beneficiários visados. Se essa lista não for já publicada através de comunicação

[10] A exceção são aqueles com privilégios e imunidades.

comunitária, é bom compreender por que as autoridades podem precisar dessa lista e uma negociação pode ser necessária para limitar os dados pessoais fornecidos.

- **Coordenação para evitar a duplicação de assistência.** Numa emergência, normalmente o governo também tem programas para apoiar as comunidades afetadas. Se houver diferentes agências que fornecem assistência, as unidades do governo podem assumir a coordenação para garantir que não haja uma duplicação da assistência e apoiar às agências para entregarem a assistência o mais rapidamente possível. Em alguns países e contextos, o governo pode solicitar dados de beneficiários a todas as organizações para comprovar a duplicação e, em alguns casos, pode inclusive ter de validar a lista antes que a organização possa proceder com a distribuição. A intenção de evitar a duplicação pode ser razoável e requer que o governo conheça os nomes dos beneficiários. Porém, não é necessário compartilhar outros dados pessoais com este fim. Também, em geral não há necessidade de facultar o acesso ao governo a sua base de dados. Quando for possível, é bom negociar, a fim de minimizar os dados compartilhados com as autoridades para facilitar a coordenação e as comprovações de duplicação.
- **Associação para a implementação.** A Sociedade Nacional pode estar numa associação com o governo para fazer distribuições em nome do governo. Pode haver programas de proteção social e amplas distribuições nos quais o governo pode se apoiar no alcance e a capacidade da Sociedade Nacional. Nessas associações, geralmente estabelece-se um acordo formal. Na negociação desses acordos, há que ter em mente os princípios e as boas práticas de proteção de dados.

Independentemente da finalidade oficial, duas questões essenciais devem ser consideradas. Em primeiro lugar, nalguns contextos, é concebível que os dados pessoais, uma vez compartilhados, possam ser usados com outras finalidades. Em segundo lugar, mesmo que só uma quantidade muito limitada de dados pessoais seja compartilhada, possivelmente esses dados possam ser combinados com outros dados que o governo já dispõe. As consequências que isso pode ter para os beneficiários são difíceis de prever. Para limitar esses dois riscos, pode ser uma opção apresentar somente uma cópia da lista de beneficiários. Os dados não digitalizados são mais difíceis de reutilizar. Ainda melhor seria se se mostrasse a lista numa reunião e levar consigo a cópia. Depende do contexto que o governo venha aceitar essa abordagem ou não, mas a ideia é tentar opções para minimizar a partilha de dados.

Quando devem ser fornecidos dados pessoais ao governo, lembre-se do seguinte:

- Ser claro em relação à finalidade da partilha de dados e às potenciais consequências para os beneficiários; mitigar sempre que for possível e identificar uma base legítima.
- Estabelecer um contrato de partilha de dados, se for viável. Esse contrato descreve formalmente a finalidade para a qual os dados pessoais são compartilhados e limita o uso dos dados a essa finalidade. Também requer que o destinatário mantenha a segurança dos dados pessoais e não os conserve durante mais tempo do necessário. Consulte o modelo de FSF da FICV[11] no tocante à orientação geral. A Sociedade Nacional tem um papel auxiliar do governo, que pode ser importante na negociação dos contratos de partilha de dados.
- Informar aos beneficiários de que os dados serão compartilhados com o governo e explicar o motivo. Ser claro sobre quais são os ministérios com os quais os dados serão compartilhados. Isso permite dissuadir certos beneficiários de compartilhar seus dados e deve ser abordado pelo programa.

[11] Pode-se encontrar um modelo de contrato com os FSFs na seção de referências desta orientação.

Decisão do Projeto 2: Que dados devo compartilhar com outras ONGs?

Minimização de Dados, Necessidade e Segurança dos Dados

Decisão do Projeto reformulado: É necessário compartilhar dados pessoais com as outras ONGs e pode isso ser feito de forma segura?

Compartilhar informações com outras ONGs pode ser necessário em alguns contextos. O seguinte são alguns exemplos, e as considerações essenciais de proteção de dados devem incluir as seguintes perguntas:

- É do interesse dos beneficiários que os seus dados sejam compartilhados?
- Será que isto exporia os beneficiários a um risco?
- Posso garantir que os dados vão ser mantidos em confidencialidade e não vão ser compartilhados com outros sem a minha aprovação?
- A outra organização tem normas de proteção de dados suficientes?

Em qualquer caso, compartilhar mais do que os nomes e os dados de contato é problemático. Os indicadores de vulnerabilidade tendem a ser muito privados e, quando for possível, os beneficiários devem ter a possibilidade de decidir com quem querem compartilhar esses dados.

Para a coordenação. A partilha de dados pressupõem que há vários atores humanitários que fornecem simultaneamente AMV e é necessário trabalhar de forma coordenada (tais como grupos locais que trabalham com dinheiro). Quando há diferentes programas em curso em simultâneo, é importante evitar a duplicação e assegurar-se de que nenhum dano é feito devido às ações dos diversos atores. Alguns esforços de coordenação visam harmonizar as quantidades das subvenções monetárias, os critérios de condução das abordagens. Apesar dessas intenções razoáveis, é aconselhável ter um olho crítico e considerar se é realmente necessário compartilhar dados pessoais e até que ponto serve para coordenar o trabalho. Com frequência é uma boa alternativa compartilhar informação geral e dados agregados (critérios de direcionamento, áreas geográficas visadas, número de pessoas apoiadas, percentagem de maiores ou crianças, quantidade da subvenção monetária, etc.). Mesmo que o objetivo é evitar a duplicação, não é automaticamente necessário comparar as listas de beneficiários. Em função do contexto, a duplicação pode ser evitada por meio da alocação de diferentes áreas de atividade (vila A/vila B) ou diferentes grupos-alvo (mulheres grávidas/maiores). Quando se conclui que a partilha de dados dos beneficiários é inevitável, a proteção de dados requer limitar ao mínimo a quantidade de dados compartilhados. Por exemplo, pode ser suficiente comparar as listas de beneficiários num papel numa reunião comum com as outras ONGs. Isto é um risco menor do que outorgar as outras ONGs acesso a sua base de dados ou enviar as listas por correio eletrónico.

Aproveitamento da experiência e do alcance numa comunidade. Nalgumas situações, uma ONG pode ter conhecimento especializado de um sector ou de grupos de uma comunidade (tais como grupos que visam mulheres e crianças vulneráveis). Neste caso, a Sociedade Nacional terá de colaborar com essas ONGs para se beneficiar da sua experiência ou conhecimento da comunidade. Muitas vezes, outras ONGs apoiam-se na Sociedade Nacional local devido à sua presença nas várias comunidades, sendo às vezes o único ator humanitário presente ali.

Também pode haver situações nas quais outras ONGs pretendem estabelecer um projeto próprio baseando num conjunto de dados de beneficiários preexistente da Sociedade Nacional. Isto é prático e poupa tempo na recolha de dados. Contudo, isto envolve um uso complementar dos dados pessoais que podem não ser compatíveis com a finalidade original da recolha de dados. Mesmo que isto pareça mais conveniente na perspetiva dos beneficiários porque podem receber mais assistência, a partilha

de dados é uma exceção, não a norma, e é aconselhável ser cauteloso.

Associação para a implementação. A partilha de dados também é importante nas associações para a implementação nas quais uma organização pode ser contratada para fornecer assistência/serviços em nome de outra organização ou para partilhar responsabilidades na implementação da AMV; por exemplo, a agência de refugiados da ONU, que trabalha com várias ONGs que fornecem serviços a refugiados. Nessas associações, a partilha de dados é normalmente negociada e incluída num contrato ou acordo. Nessas negociações, é importante avaliar os riscos para os beneficiários quando os dados são compartilhados e geridos por sócios, assim como as funções e as responsabilidades dos sócios e as responsabilidades compartilhadas no tocante à proteção de dados. É possível que a agência principal possa estabelecer as normas de proteção de dados, mas se a avaliação de riscos verificar lacunas ou se considerar que algumas disposições devem ser reforçadas, não duvide em comunicá-lo ao seu diretor e/ou discutir com a equipa da sua Sociedade Nacional para que possa ser abordado no processo de negociação. Por exemplo, se a Sociedade Nacional recolher dados dos beneficiários, é preciso entregar todos esses dados ao sócio principal ou os dados podem ser minimizados no essencial para cumprir as responsabilidades na associação? Se tiver vários programas de AMV paralelos que visam aos mesmos beneficiários de acordo com o contrato da associação para a implementação, como garantir a separação do acesso dos sócios a elementos fora do âmbito do contrato?

Plataforma comum. Há várias iniciativas para desenvolver uma plataforma comum para a partilha de dados dos beneficiários e que potencialmente use o mesmo mecanismo de pagamento por várias organizações participantes. Isto requer uma base de dados ou um mecanismo para obter a interoperabilidade dos sistemas de dados propriedade das agências para a partilha e exposição do conjunto acordado de dados dos beneficiários. Essa plataforma visa melhorar a coordenação e a colaboração entre os atores humanitários e pode ser apoiada por alguns doadores, pois pode melhorar a eficiência. Existem várias abordagens para obter essas plataformas comuns e a Sociedade Nacional deve avaliar de novo as necessidades e os riscos para os beneficiários antes das ganâncias de eficiência para as organizações. Algumas questões para considerar:

- É essa plataforma absolutamente necessária para a Sociedade Nacional fazer transferência monetária? Existem diferentes formas de coordenar e colaborar com outras ONGs que podem não requerer o acesso direto aos dados dos beneficiários.
- Que dados são requeridos para constar na plataforma comum, e podem ser minimizados?
- Como os beneficiários devem ser informados quando os seus dados forem usados por outras agências? E quem deve informá-los?
- Uma vez que os dados foram compartilhados através da plataforma comum (ou seja, quando as outras agências tiverem acesso aos seus dados), como garantem os sócios que os dados serão usados para as finalidades acordadas?
- Quais são as características de segurança da plataforma para garantir que unicamente pessoal autorizado possa ter acesso aos dados?
- Qual seria a regência do acesso de dados pelas diferentes ONGs? Quantas mais ONGs participarem, mais complicado é de gerir. Em particular, quando uma organização decide deixar de participar na plataforma comum, como seriam usados doravante os dados que essa organização compartilhou?
- Onde serão conservados os dados, e levanta esse lugar (por exemplo, fora do país alvo) questões de cumprimento da proteção de dados?

Se a decisão de compartilhar dados pessoais com outras ONGs for tomada, em primeiro lugar é

importante estabelecer um contrato. A base legítima para o tratamento deve ser identificada. Quando a partilha de dados for realizada através de uma plataforma comum, esse contrato tem de ser ainda mais sólido, com normas de proteção de dados sólidas, e com o âmbito e as obrigações e responsabilidades dos sócios participantes bem definidos. Recomenda-se implicar os técnicos das TI e especialistas legais na negociação do contrato relativo à plataforma comum para garantir um nível de proteção suficiente. Em segundo lugar, os beneficiários devem ser informados de que os dados serão compartilhados com outras agências. Se a partilha de dados não estiver prevista no momento da recolha ou do registo, será difícil informar a cada pessoa. Em tal caso, informar a aqueles beneficiários será a responsabilidade da outra ONG que vai usar os dados compartilhados por você. É aconselhável deixar isso claro no contrato de partilha de dados.

Decisão do Projeto 3: Que dados devo compartilhar com os doadores?

Minimização de Dados, Necessidade e Segurança dos Dados

Decisão do Projeto reformulado: É necessário e seguro compartilhar dados pessoais com doadores?

Para os doadores é importante garantir a responsabilização e a transparência nas suas atividades de financiamento e, portanto, é possível que peçam para compartilhar alguns dados de beneficiários. De novo, é importante pensar nos potenciais riscos para a privacidade dos beneficiários e considerar opções para limitar a quantidade de dados compartilhados.

São duas as principais finalidades para os doadores pedirem e usarem dados dos beneficiários:

- **Para obter compreensão do programa e monitorar a situação.** Geralmente o doador quer entender as circunstâncias no terreno e como a equipa do programa está a responder. Normalmente basta fornecer informações gerais e dados agregados (critérios de seleção, áreas, número de pessoas apoiadas, percentagem de maiores/crianças, quantidade da subvenção monetária, etc.). Compartilhar detalhes dos nomes e outros dados pessoais não é normalmente necessário. O doador também pode ter interesse em saber como os beneficiários aplicam o dinheiro que recebem.[12] De novo, os dados agregados deveriam bastar (por exemplo, percentagem de pessoas que gastam dinheiro em alimentos ou outros produtos básicos, percentagem de pessoas que mantiveram o dinheiro mais de uma semana, etc.).
- **Para cumprir requisitos de auditoria.** Com frequência, o doador requer dados beneficiários para cumprir requisitos de auditoria. Os doadores devem assegurar-se de que o dinheiro doado é efetivamente usado para a finalidade prevista. Outras auditorias comprovam se os beneficiários são pessoas reais que cumpriam os critérios de direcionamento acordados e que efetivamente receberam a assistência monetária (prova de receção). Para essas atividades ligadas a auditorias, existem diferentes opções para proteger a privacidade dos beneficiários:

  Ao **compartilhar uma lista** para realizar as comprovações, os dados incluídos podem estar limitados ao mínimo necessário, e, potencialmente, em vez de expor os nomes dos beneficiários, podem ser usadas identificações únicas de referência. Por exemplo, para uma prova de receção, o nome, a data e a assinatura mostrando que receberam o dinheiro deveria bastar. Em alguns casos, inclusive o nome pode não ser necessário sempre que a identificação do beneficiário for fornecida. Se as assinaturas forem

[12] Note-se que este tipo de informação não deve ser recolhido de forma automática. Deve existir uma base legítima para a recolha de informação sobre as compras realizadas pelos beneficiários. Antes de recolher essa informação, que pode revelar dados sensíveis sobre os beneficiários, é preciso realizar uma revisão de proteção de dados. Ver capítulo sobre Monitoramento Após Distribuição.

[13] É importante considerar questões tais como os requisitos de auditoria na fase de negociação do contrato.

recolhidas num papel que contenha mais informações do que as necessárias, as respetivas colunas devem ser eliminadas, retiradas ou apagadas antes de serem enviadas ao doador, a fim de aumentar a proteção de dados.

Outra abordagem é **outorgar acesso limitado no tempo e à leitura** à base de dados ou à documentação, para assim os auditores fazerem as suas comprovações. Os auditores dos doadores podem verificar os dados ou a documentação relevantes em pessoa junto consigo, sem descarregar nem levar nenhum dado consigo. Pode discutir com o doador com antecedência quais informações são necessárias e os métodos para realizar essas comprovações. A partilha de dados com os doadores deveria ser incluída no contrato ou acordo com eles.[13] A base legítima deve ser identificada, e os beneficiários devem ser informados sobre a partilha de dados prevista com os doadores.

VII. Monitoramento Após Distribuição

Uso de Dados Pessoais

Para compreender se os objetivos do programa de AMV estão a ser cumpridos, é precisa uma estratégia de monitoramento e avaliação. Parte desta estratégia é determinar os indicadores necessários para identificar realizações, resultados e impacto, assim como a metodologia para obter e analisar esses indicadores. Existem vários tipos de monitoramento, incluindo monitoramento de mercado, monitoramento de referência, monitoramento de receção (que geralmente usa pesquisas de saída) e monitoramento após distribuição. Para esta secção, vamos nos focalizar no monitoramento após distribuição (MAD). Para mais detalhes sobre monitoramento e avaliação, ver Módulo M5 2 Monitoramento do Programa no *kit* de ferramentas de AMeE.

É importante para as organizações humanitárias e os doadores saberem como e quando os beneficiários usam o dinheiro que recebem. Geralmente os MAD realizam-se algumas semanas depois da distribuição monetária, a fim de permitir aos beneficiários usarem o dinheiro recebido. Os MAD são úteis para avaliar a qualidade do programa e melhorar futuros programas de assistência monetária e é provável que façam uso de dados pessoais. Em função do programa, poderia haver várias visitas aos beneficiários para monitorar o avance (por exemplo, construção de abrigos como parte da recuperação), onde diferentes conjuntos de dados deverão ser monitorados no tempo.

Considerações de Proteção de Dados

A palavra “monitoramento” pode indicar que os beneficiários estão a ser controlados de um certo modo e o seu comportamento analisado. Porém, realmente, não é o beneficiário, mas sim o programa e a sua efetividade que estão a ser monitorados. Contudo, isso não quer dizer que o monitoramento (do programa) não terá consequências para o beneficiário. Assim, a privacidade dos beneficiários deve ser considerada.

Note-se: As Decisões do Projeto deste capítulo focalizam-se no MAD. Para o monitoramento de referência e de receção, o aspeto essencial é a minimização de dados/necessidade. Ao recolher dados dos beneficiários, é importante pensar em quais são os dados realmente necessários no contexto do monitoramento do programa. Ao usar modelos padronizados, devem ser adaptados ao contexto por meio da eliminação das questões desnecessárias. Consulte de novo os capítulos sobre Direcionamento e Registo de Beneficiários. Outro método recomendado para aumentar o nível de proteção de dados no monitoramento de referência e receção é a retirada da identificação direta dos beneficiários (como nomes e identificações pessoais).

Decisão do Projeto 1: Quais dados pessoais devo recolher no processo de monitoramento?

Minimização de Dados, Necessidade

Decisão do Projeto reformulado: Como limitar o uso de dados pessoais no processo de monitoramento?

Em função do contexto, o monitoramento pode ser feito em diferentes formas. Examinaremos o MAD em relação às transferências condicionais e incondicionais e às considerações de proteção de dados.

Condicionalidade e Restrição

O pograma de AMV pode ter certa *condicionalidade* (requisito prévio que os beneficiários devem cumprir antes de receber o dinheiro, tal como a assistência à escola, a promoção da saúde, *workshop* sobre meios de subsistência) ou *restrições* (requer os beneficiários usarem a assistência para elementos ou serviços específicos ou lograrem um resultado, como a reparação de abrigos ou o início de meios de subsistência). O objetivo do monitoramento é comprovar se as condições se mantêm cumpridas e as restrições estão a ser respeitadas ao longo do tempo. Uma consideração essencial é a privacidade dos beneficiários. Isto pode ser feito reduzindo a quantidade de informações recolhidas ao absolutamente necessário. Além disso, é útil estabelecer intervalos de tempo razoáveis para o monitoramento e limitar o número de pessoas envolvidas no monitoramento dos mesmos beneficiários. Também, é aconselhável limitar o acesso aos dados desagregados, que podem ser usados por diferentes partes interessadas ou envolvidas no processo de monitoramento.

Exemplo:

No contexto de um programa, os beneficiários devem usar a assistência recebida para construir um abrigo após um furacão devastador. A equipa do programa decide visitar cada beneficiário após uma semana e de novo após três semanas, para comprovar como está a avançar a reconstrução do abrigo. A equipa perguntará sobre os materiais comprados com a assistência monetária e comprovará visualmente o avance do abrigo. Não pedirá para o beneficiário preencher largos formulários sobre as suas condições de vida gerais nem tomará uma foto da construção. A equipa também decidiu ter duas equipas de monitoramento separadas abrangendo diferentes áreas geográficas. As mesmas equipas vão monitorar as mesmas famílias após três semanas para garantir a consistência do monitoramento, pois não são tomadas fotos, e assim os mesmos membros da equipa podem verificar o avance da construção.

Incondicional e irrestrito

Quando o dinheiro for entregue aos beneficiários para gastarem nas suas necessidades específicas e não num produto ou atividade predefinidos, o monitoramento pode ser diferente. Os dados dos beneficiários serão ainda necessários para comprovar como (em termos gerais, por exemplo por categoria) têm gastado a assistência recebida e se os objetivos do programa foram cumpridos. A intenção não é monitorar os beneficiários individuais, mas entender a efetividade do programa. O comportamento global dos beneficiários participantes é um indicador importante para avaliar se os critérios de direcionamento e a quantidade do dinheiro outorgada foram apropriados.

O método típico de monitoramento é estabelecer Discussões de Grupo Focal com uma amostra dos beneficiários e não beneficiários da comunidade. Faz-se uma discussão oral com essas pessoas sobre o projeto em geral. Pergunta-se geralmente sobre a sua opinião sobre o projeto (os critérios de direcionamento, os efeitos do projeto, etc.) Além disso, são convidados a socializar as suas

experiências sobre como o dinheiro tem sido usado. Numa perspetiva de proteção de dados, as discussões orais enquanto tal são menos problemáticas do que a recolha formal de informações no papel ou no formato digital. Contudo, deve-se considerar atenciosamente como são registradas as DGFs. As gravações de vídeo e áudio podem interferir fortemente com a privacidade dos participantes. Em geral, é preferível tomar atas das reuniões. Provavelmente, isto também facilitará que os participantes expressem a suas experiências e opiniões. Ao tomar atas das reuniões, existem opções para aumentar o nível de privacidade. Pode-se considerar a limitação das notas no seguinte:

- Pontos de discussão gerais – em vez de salientar os comentários individuais das pessoas.
- Número de participantes e características essenciais que fazem deles bons exemplos (idade, género, área de residência) em vez de registar os nomes completos.

Ainda assim, é possível que os comentários não sejam completamente anónimos. As pessoas que tomam parte na discussão sabem quem foi que disse uma coisa. Contudo, para as pessoas que consultarem as notas da reunião, será mais difícil identificar à pessoa individual atrás de um certo comentário. Naturalmente, dependerá do contexto se essa informação limitada é suficiente aos efeitos do monitoramento.

Outro método de monitoramento é fazer entrevistas com uma amostra dos beneficiários. Isto faz-se geralmente com modelos de questionários. Será importante comprovar a identidade do beneficiário entrevistado para se assegurar que é a pessoa correta e que efetivamente recebeu a assistência monetária. Porém, pode não ser necessário conservar essa informação sobre a identidade, e assim um certo nível de anonimidade pode ser mantido. O entrevistador conhecerá a identidade do beneficiário, mas os dados produzidos após o preenchimento do questionário terão maior proteção face a outras pessoas que consultarem os dados.

Exemplo:

A equipa do programa solicita uma amostra de beneficiários para participarem num MAD para determinar como foi usada a assistência monetária.[14] A equipa comprova as identificações dos participantes, mas não as regista, nem os nomes, no formulário. Na pesquisa, os beneficiários foram sinceros em relação à sua insatisfação com a forma de receção, pois tiveram que viajar longe para encontrar um agente monetário, houve problemas de liquidez com o agente e disseram que teria sido útil receber assistência em espécies e não monetária. Devido ao respeito à sua privacidade, em vez de dizerem superficialmente que estavam satisfeitos por medo de não receber a assistência de novo, foram sinceros e isso permitiu à equipa aprender e fazer mudanças para o seguinte desembolso.

Se não for factível manter a anonimidade da identidade dos beneficiários nos questionários, é importante limitar as perguntas ao mínimo necessário. Os modelos tendem a incluir um vasto leque de perguntas que abrangem vários cenários (questionário único válido para todos os casos). Tal como se explica no capítulo sobre o Registo, esses modelos padronizados devem ser adaptados às circunstâncias específicas conforme necessário. As perguntas desnecessárias devem ser apagadas ou eliminadas.

Tente encontrar opções para evitar o uso dos dados pessoais. Se os dados pessoais forem usados para

[14] Note-se que os beneficiários devem fornecer as informações de forma voluntária; não podem ser forçados. Deve ficar claro que a sua participação não afetará às distribuições em curso nem futuras e que são livres de recusar-se a participar.

efeitos do monitoramento, é importante identificar a base legítima para o monitoramento e informar ao beneficiário do tratamento dos dados no contexto do monitoramento.

Decisão do Projeto 2: Que dados os beneficiários podem-me entregar o FSF para monitorar o programa?

🔔 Minimização de Dados, Necessidade e Confidencialidade dos Dados

Decisão do Projeto reformulado: Que dados pode o FSF entregar-me para os efeitos de monitoramento sem invadir a privacidade dos beneficiários?

Quando os programas monetários usarem FSF, os fornecedores podem ter dados sobre os beneficiários que podem ser úteis no processo de monitoramento. Em função do FSF, podem incluir alguns dados: quando o dinheiro for retirado e onde (por exemplo, num caixa multibanco ou agente monetário), se o dinheiro for usado para comprar numa certa loja (por exemplo, mercearia ou loja de bebidas) e a assinatura na prova de receção. Obter esses dados pode ajudar a acelerar o processo e obter informações precisas sobre o processo de monitoramento. Contudo, numa perspetiva de proteção de dados, essa abordagem pode apresentar certos riscos. Os dados ligados aos pagamentos e às compras poderiam ser bastantes sensíveis. Recolher esses dados de uma fonte indireta (o FSF) e não diretamente dos beneficiários poderia ser considerado como uma interferência na privacidade deles.

Contas pessoais dos beneficiários

Quando a distribuição for feita através de contas pessoais (banco/móvel) dos beneficiários, por defeito a Sociedade Nacional não tem acesso a essas contas. No entanto, o FSF pode rastrear os movimentos da conta e pode estar disposto a compartilhar consigo os dados de pagamento. Portanto, a questão é se isso é relevante e que é necessário para o objetivo do monitoramento? Pode até querer entender quando e como o dinheiro foi usado. No entanto, o foco do monitoramento não é no beneficiário individual, mas no comportamento global de todos os beneficiários. Portanto, geralmente bastará com receber informação agregada dos pagos. Por exemplo, o FSF poderia indicar-lhe:

- A percentagem de beneficiários que gastaram o dinheiro na primeira semana;
- A percentagem de beneficiários que gastaram o dinheiro nas lojas específicas, como supermercados ou farmácias;
- O tempo médio no qual os beneficiários usaram o dinheiro integralmente;
- As regiões nas quais o dinheiro for gasto mais rápido;
- A localização relativa dos agentes monetários e quais entregaram mais dinheiro do que os outros;

Em função do contexto do programa, pode acordar com o FSF que informações devem fornecer-lhe, considerando o princípio de minimização dos dados e da necessidade.

Exemplo:

Um programa monetário entrega dinheiro através de cartões pré-pago, que os beneficiários podem usar para comprar nas lojas e estabelecimentos que aceitem MasterCard ou retirar dinheiro de um caixa multibanco. A Sociedade Nacional deseja entender para que categorias de produtos básicos foram aplicadas o dinheiro e comprovar com o FSF se essas informações puderem ser fornecidas. A equipa do programa solicita especificamente os dados agregados e a visualização se (1) o dinheiro foi usado mais para retirar dinheiro de caixas do que para comprar, (2) a percentagem dos beneficiários que ainda não tiverem usado a assistência monetária e (3) as categorias das lojas onde os cartões foram usados (tais como produtos alimentares, medicamentos, serviços). O FSF só compartilha os dados agregados e as visualizações relevantes, em vez de dados específicos sobre as compras e que pessoas operaram e quando.

Na prática, e se não for previamente negociado, o FSF poderia não estar disposto a criar informações específicos ou entregar informações demasiado específicas, pois é um esforço adicional. Se for o caso, outra opção é pedir ao FSF **não** lhe enviar o conjunto completo de dados de pagamento e só informação transacional muito limitada para proteger a privacidade dos beneficiários. Deve-se pedir para o FSF eliminar os nomes e os números dos cartões de cada atividade financeira.

Se a única opção é receber os dados transacionais brutos e completos do FSF, é aconselhável limitar quem recebe e tenha acesso aos dados completos e fazer que essa pessoa seja o "guardião" na sua equipa. O FSF enviará os dados de pagamento somente a essa pessoa. O guardião pode então extrair somente as informações necessárias para o processamento do resto da equipa do programa. O guardião pode então eliminar os dados completos recebidos pelo FSF com segurança, a fim de que não sejam usados acidentalmente para outra coisa. A informação agregada abstrata oferece um maior nível de proteção de dados e em muitos casos pode ser suficiente.

Exemplo:

O programa monetário distribui dinheiro através dos porta-moedas móveis dos beneficiários. A Sociedade Nacional gostaria de entender que agentes de dinheiro móvel foram usados para a receção monetária, para poder informar aos fornecedores antes da seguinte distribuição em caso de problemas de liquidez. O FSF não é capaz de fornecer essa informação somente, mas está disposto a enviar a lista completa de transações com todas as atividades financeiras de cada beneficiário individual e onde foram realizadas. A equipa do programa informa ao FSF que deve enviar essa informação somente ao diretor de Gestão da Informação que gere o programa monetário, que depois extrairá os dados necessários para o processamento pela equipa do programa. O diretor de Gestão da Informação elimina o arquivo após extrair só os dados agregados requeridos pela equipa.

Conta virtual da Sociedade Nacional

Quando a distribuição for feita através de contas virtuais da Sociedade Nacional (ver capítulo sobre o FSF), o FSF pode não ter nenhuma ligação direta entre os dados transacionais e os beneficiários efetivos, já que a gestão da subconta é realizada pela Sociedade Nacional. Consequentemente, o facto de uma pessoa ter acesso direto às transações dos beneficiários porque é o titular da conta pode representar alguns riscos à privacidade. Tal como foi discutido, os dados individuais de pagamento individual são sensíveis e, para efeitos de monitoramento, normalmente não é necessário saber nada sobre os beneficiários individuais, mas sobre o grupo dos beneficiários em conjunto.

Uma opção para proteger de novo a privacidade dos beneficiários é designar um "guardião", que será o único com acesso as transações completas disponíveis na plataforma. Se só uma pessoa da equipa tiver acesso à plataforma e transformar a informação individual em informação abstrata, o risco de proteção de dados pode ser reduzido. Quando não for possível designar um guardião, é a responsabilidade de todos os membros da equipa que tenham acesso à plataforma e ao conjunto completo de dados respeitar a confidencialidade e privacidade dos beneficiários e se assegurar de que os identificadores das subcontas não estejam ligados de volta às pessoas, por isto é essencial que todos os membros da equipa tenham uma boa familiaridade com as práticas e os princípios de proteção de dados.
Tente monitorar o programa sem receber os dados pessoais dos beneficiários do FSF. Sempre que receber esses dados, é importante informar ao beneficiário sobre isto e explicar como pretende proteger a privacidade dos beneficiários.

Decisão do Projeto 3: Que dados dos beneficiários podem entregar-me o negociador num programa de assistência através de vouchers?

Minimização de Dados, Necessidade e Segurança dos Dados

Decisão do Projeto reformulado: Que dados podem entregar-me o negociador para efeitos de monitoramento sem invadir a privacidade dos beneficiários?

Nos programas baseados em vouchers, os dados das transações dos negociadores podem ser usados no monitoramento. O negociador terá registos sobre quantos vouchers foram convertidos em qual prazo, e também terá registos dos produtos básicos selecionados em troca dos vouchers. No entanto, ainda assim é importante garantir um elevado nível de proteção de dados no uso dessa informação. Em geral, é suficiente rever dados agregados sobre o uso geral dos vouchers e os produtos básicos comprados. Para efeitos de monitoramento, não é relevante para que um beneficiário individual usou o voucher. O que é importante é entender o comportamento global dos beneficiários participantes para avaliar a efetividade do programa. Portanto, deveria evitar-se a revisão de dados que permitam identificar quando e como um beneficiário individual comprou um certo produto. Isto pode ser feito solicitando ao negociador a agregação dos dados. Se não for possível, solicite somente um conjunto de dados limitados sem identificadores. De outro modo, como indicado nas anteriores seções, tente designar um "guardião" na sua equipa, que receberá e extrairá o conjunto relevante de dados, e imediatamente elimine a lista de transações completa.

VIII. Orientação Geral

Este capítulo examina as considerações essenciais de proteção de dados que sejam aplicáveis durante o programa monetário.

Considerações de Proteção de Dados

Armazenagem de Dados

Ao recolher dados pessoais dos beneficiários, é extremamente importante manter a sua segurança e protegê-los. Isto envolve tomar medidas de segurança suficientes para evitar a chamada vulneração de dados (perda, acesso não autorizado, etc.) (consultar abaixo a orientação sobre o que fazer em caso de vulneração de dados).

As soluções de TI para a segurança dos dados são muito técnicas e com frequência requerem conhecimento de especialistas. Portanto, recomenda-se desenvolver uma abordagem coerente para todos os programas junto com o seu Diretor de TI, se for possível. O conceito pode abordar fluxos de dados, os canais e as interfaces para a troca de dados, os níveis de encriptado quando os dados são conservados e transferidos, *backup* ou armazenagem redundante para impedir a perda de dados, e os controlos de acesso para garantir que somente as pessoas autorizadas estejam a usar os dados, etc.

Em qualquer caso, os seguintes aspetos devem ser atenciosamente considerados:

- Para os dados digitais, sempre que for possível, é essencial usar uma base de dados ou uma solução de gestão de dados sólidas. A conservação de dados em repositórios publicamente disponíveis, como Google ou Dropbox, deve evitar em todas as circunstâncias. O uso de bases de dados tem muitas vantagens, já que oferecem segurança técnica, como criptografia nativa, repositórios/pastas protegidos por senha, rastreio de arquivos de *log*, *backups*, etc. As soluções de gestão de dados (tais como RedRose e LMMS) podem integrar-se com diferentes ferramentas de recolha de dados, tais como ODK/Kobo, e mecanismos de pagamento, como dinheiro móvel ou bancos para transferência monetária. É importante avaliar essas soluções em termos de segurança de dados para garantir que os dados sejam protegidos, tanto em trânsito (por exemplo, quando no uso de recolha de dados móveis, como ODK/Kobo, os dados são carregados desde o telemóvel ao servidor de gestão de dados) ou em repouso (quando os dados são armazenados no servidor na nuvem). A localização física de armazenagem dos dados também deve ser avaliada com respeito às leis nacionais (ou seja, alguns países proíbem ou colocam limitações à transferência de dados pessoais fora da sua jurisdição).
- Quando os dados devem ser conservados no computador ou dispositivos USB, o risco de perda e roubo é maior do que na própria base de dados. Devem adotar-se medidas de segurança adicionais para limitar esse risco. Idealmente, o *hardware* deve ser protegido através de encriptação de discos rígidos (tal como Bitlocker de Microsoft). Além disso, pode adicionar um nível adicional de proteção através da encriptação ou protegendo por senha os documentos no disco rígido. Os computadores e dispositivos USB também devem ser segurados fisicamente através do uso de senhas no computador e sendo armazenados numa gaveta travada quando não estiverem em uso.
- Na criação de senhas, tente usar senhas robustas que não sejam fáceis de adivinhar. A boa prática é usar maiúsculas e minúsculas, dígitos e carateres especiais e mudar a senha de forma regular. Evite compartilhar as contas e as senhas. Se a conta for genérica (por exemplo, caixas postais eletrónicas genéricas geridas por múltiplas pessoas), é importante limitar o número de pessoas (ver abaixo – Controlo de Acesso).
- Os arquivos de papel têm um risco ainda maior de perda e de acesso não autorizado. Se os arquivos de papel forem a única opção, deverão ser conservados num espaço com fechadura. Isso ajuda a limitar o acesso de terceiros.

Para mais dicas, ver o Folheto de Proteção de Dados de Gestão da Informação da FICV que indica o que se deve fazer e o que não diz respeito à armazenagem e ao tratamento e a política de segurança da informação da FICV.

Conservação e Eliminação dos Dados

O que acontece com os dados pessoais dos beneficiários uma vez que o programa for completado? Idealmente, não são deixados em arquivos em papel nem numa base de dados por um tempo ilimitado. Uma vez que os dados de um programa específico não são mais necessários, devem ser eliminados, ou como mínimo agregados ou anonimizados. Se forem necessários por um período maior, mas não se requer um acesso regular (como nas auditorias), o arquivado de forma *offline* e segura pode ser uma opção.

Períodos de Conservação

Recomenda-se estabelecer previamente um período de conservação limitado no tempo, definindo durante quanto tempo os dados devem ser conservados normalmente. Uma vez que o período de conservação expire, os dados são eliminados. Somente se houver motivos imperiosos que requeiram

uma maior conservação, os dados poderão ser conservados durante um período maior, mas limitado.

Os períodos de conservação podem ser incorporados às bases de dados, para permitir a eliminação automática dos dados. Se quiser aprender mais sobre essas opções, consulte com os colegas de TI da sua organização. Se as bases de dados ou os períodos de conservação automáticos não puderem ser usados, outra opção é estabelecer lembretes. O objetivo é refletir de forma ativa e a intervalos periódicos sobre se manter ou destruir os dados que já não sejam necessários. A duração dos períodos de conservação depende do próprio programa, mas também poderia ser estabelecido pelas políticas da própria organização. No desenho da intervenção de AMV, os períodos de conservação apropriados devem ser considerados, a fim de que possam ser comunicados aos beneficiários. Alguns aspetos para considerar são os seguintes:

- A duração do projeto;
- A sensibilidade dos dados;
- A escala do monitoramento planeado;
- A probabilidade de haver questões de seguimento;

Outras finalidades

Mesmo que o programa tenha sido terminado e que o monitoramento tenha sido completado, pode parecer útil manter certos dados para outras finalidades. Em primeiro lugar, poderiam ser usados para criar **informações e estatísticas** adicionais. Contudo, geralmente para este fim não é necessário manter dados que identifiquem às pessoas diretamente (tais como nomes ou números de identificação). É suficiente gerar um conjunto condensado de dados agregados. Em segundo lugar, em particular para as áreas suscetíveis aos mesmos perigos, é provável que os dados possam ser úteis para a **preparação geral de futuros programas e similares** (por exemplo, furacões ou tufões recorrentes). Nessas situações, pode parecer razoável simplesmente manter os dados. Contudo, os dados tendem a ter um ciclo de vida limitado. Para os novos programas, deverão ser atualizados e verificados. As pessoas partem ou deslocam-se a outra área, as suas condições de vida mudam, crianças nascem, ou membros da família morrem. Por isso, frequentemente a conservação dos dados para um novo programa potencial não é útil. Se decidir manter os dados para um programa futuro, também é importante considerar se a nova finalidade é compatível com a finalidade original. As finalidades humanitárias podem ser compatíveis, mas se a finalidade não for compatível, é essencial informar aos beneficiários sobre a sua intenção de usar os dados de novo para outro fim e identificar uma nova base legal para esse novo tratamento (ver a seção sobre Base legítima no capítulo de Registo). Em terceiro lugar, os dados poderão ser conservados para **efeitos de auditoria**. Se for o caso, normalmente os requisitos de auditoria estabelecem períodos de conservação requeridos. Se não for o caso, com frequência pode-se identificar um período de conservação razoável com base no prazo e/ou na finalidade da auditoria. Os dados conservados para efeitos de auditoria devem ser arquivados de forma separada de outros fluxos de dados.

Dados de não beneficiários

No processo de direcionamento, recolhem-se dados pessoais de pessoas que finalmente podem não receber a assistência, porque não cumprem a comprovação de elegibilidade (ver capítulo sobre Direcionamento). De forma similar, durante o registo dos beneficiários, é possível que sejam recolhidos dados de pessoas que finalmente virão a ser não elegíveis. A armazenagem de dados pessoais desses não beneficiários deve ser considerada atenciosamente. Dado que não vão participar no programa, os seus dados já não são necessários uma vez que a comprovação de elegibilidade for completada. No entanto, pode ser do seu interesse e também do interesse dos não beneficiários manter a informação pessoal durante um certo período de tempo. Um motivo pode ser provas das decisões no caso que um não beneficiário inicie uma queixa contra a Sociedade Nacional por ter sido

excluído do programa. Nesta situação, pode ser muito útil poder ver como isto foi decidido e quais dados foram usados nessa decisão. Se for possível, em situações como esta, a informação respetiva deve ser conservada de forma separada do resto dos outros beneficiários elegíveis. A ideia é que esses dados já não fazem parte do fluxo de dados do programa em curso, mas se uma queixa for apresentada, podem ser recuperados.

Controlo de Acesso

A informação recolhida diretamente dos beneficiários ou de outras fontes (governos, etc.) deve ser tratada de forma confidencial. A confidencialidade está estreitamente ligada aos princípios de minimização dos dados e de necessidade e segurança dos dados, tal como foi explicado acima.

Geralmente, os programas monetários implicam diferentes partes interessadas: internas (tais como as equipas diretas do programa e as equipas de terreno, serviços de apoio, como colegas de Finanças, Logística, gestão da informação e IT, e diretores) e externas (tais como FSFs, doadores, governo, outras ONGs). Já temos examinado o tratamento de dados pessoais com partes interessadas externas (ver capítulos sobre os FSFs e a partilha de dados com partes externas). Para as pessoas interessadas internas, é importante determinar o tipo de acesso e o nível de acesso requerido no tocante aos dados dos beneficiários. Algumas organizações têm uma classificação das informações. Por exemplo, a política de segurança da informação da FICV categoriza os dados dos beneficiários como confidenciais ou muito confidenciais em função do contexto; isto requer o maior nível de segurança, assim como acesso limitado com base na "necessidade de conhecer".

Algumas formas de garantir um controlo de acesso apropriado:

- Uso do nome de usuário e da senha para ter acesso a base de dados ou a plataforma de gestão de dados. Informar aos usuários de que não devem compartilhar o seu nome de usuário e senha com outros. Também é importante evitar a criação de usuários genéricos que permitem a múltiplas pessoas conectar por meio desse usuário. As ações de cada usuário deve ser auditado e rastreáveis.
- Use um controlo de acesso dependente das funções (RBAC), o que significa que se outorgam aos usuários funções específicas e cada função outorga o acesso a certas funções e dados no sistema. O acesso pode ser tão granular quanto seja necessário (como acesso à lista de beneficiários, capacidade de descarregar a lista de beneficiários, ou somente acesso a dados agregados como painéis de instrumentos). O acesso deve ser revocado se existir uma questão de segurança com um usuário.
- Ter um registo de acesso para registar qualquer pessoa que faça *login* e acesse certas páginas ou dados, assim como um registo de descarregamento daqueles que descarregam dados diretamente do sistema (indicando que isso também é considerado recolha e tratamento de dados pessoais e deve ser tratado de forma apropriada).
- Ao descarregar dados numa folha de cálculo Excel, adicionar uma proteção por senha ou encriptar o arquivo.
- Se não houver uma base de dados, os arquivos devem ser protegidos por senha e somente o pessoal autorizado deve ter acesso aos arquivos. Para os arquivos de papel, só o pessoal autorizado deve ter acesso direto e os arquivos devem ser mantidos num local com fechadura.

Exemplos:

O programa monetário envolve 10 membros do pessoal e voluntários para a sua implementação. Enquanto três são responsáveis na condução e no registo dos beneficiários (Equipe 1), os outros 7 são responsáveis de entrar em contacto com os fornecedores de serviços e da distribuição monetária (Equipe 2). A equipa 2 não precisa conhecer a vulnerabilidade dos beneficiários. Só precisa saber os dados pessoais necessários para a parte monetária do projeto (nomes, contas bancárias, KYC). Portanto, uma lista dos beneficiários com informação limitada é gerada por eles pela Equipa 1. Todas as outras informações são conservadas numa base de dados protegida por senha e somente a Equipe 1 tem essa senha. Além disso, só 1 pessoa tem a função de administrador e pode ter acesso completo à base de dados (acesso de leitura e escritura), e os dois outros membros da equipa só têm acesso a leitura.

No mesmo cenário, o método de distribuição é dinheiro em envelopes. Prevê-se que a Equipa 2 terá de justificar a eleição dos beneficiários no dia da distribuição. Se essa situação acontecer, é necessário que a Equipa 2 tenha acesso à informação complementar. Portanto, solicita a informação adicional à Equipa 1, que gera a informação limitada adicional.

Processo de Transmissão (Partilha de Dados)

Numa partilha de dados, o processo de transmissão pode aumentar o risco da perda de dados e de acesso não autorizado. Portanto, na transmissão de dados pessoais, as medidas de segurança desempenham um papel importante.

- Idealmente, os dados são compartilhados através de **ferramentas seguradas,** tais como FTP seguro com nome de usuário e senha de acesso limitado para o descarregamento de dados da base de dados segura ou da plataforma de gestão de dados.

- Quando uma comunicação relativa aos beneficiários deve ser enviada através de **email**, é importante lembrar-se de: (1) limitar o número de destinatários, (2) proteger com senha os anexos e (3) encriptar os emails (quando for possível). Isto oferece alguma proteção no caso em que os emails sejam hackeados ou enviados acidentalmente a um endereço errado. O risco de expor os dados dos beneficiários a pessoas não autorizadas se reduz quando os emails e os anexos estão encriptados. Se não tiver a certeza se os arquivos ou emails devem ser encriptados, entre em contacto com os seus colegas de TI. Enviar emails a listas de correio em vez de as pessoas pode parecer conveniente, mas pode ser problemático se não tiver conhecimento exato de quem está incluído nessas listas. Isto mesmo é certo quando emails forem enviados a endereços de email genéricos onde pode haver diferentes pessoas que tenham a senha ou gerindo a conta de email genérica. É preciso também ter cautela quando emails são reenviados ou quando cadeias de correio são criadas, com respostas de múltiplas pessoas às mensagens. À medida que os destinatários crescem ou mudam, é preciso assegurar-se de que os novos destinatários também têm autorização para ser informados dos dados pessoais dos beneficiários.

  Por exemplo:

A situação de alguns beneficiários potenciais se discute através de email com os líderes comunitários para decidirem se qualificam para o programa monetário. O email pode ser enviado ao líder comunitário que ajuda na tomada de decisões e a colegas envolvidos no processo. Contudo, deve ser evitado o envio do email a um endereço de email genérico, tal como "info@community" ou "cashteam@".

- Tome cuidado se desejar compartilhar arquivos que contenham dados pessoais através de **aplicações de mensagens móveis**, como WhatsApp. A menos que tiver confiança na segurança da app de mensagens (por exemplo, considera-se amplamente que o sinal é significativamente mais segura do que WhatsApp), **não faça uso dela** para compartilhar dados pessoais ou outros dados sensíveis (pertencentes a pessoal, voluntários ou beneficiários).

Gestão de Vulnerações de Dados

Apesar de todas as medidas de segurança, não existe a garantia de que a vulneração de dados possa ser prevenida em todas as situações. Tal como se define no início desta orientação, uma vulneração de dados *envolve o acesso não autorizado a ou a destruição, perda, alteração ou divulgação de dados pessoais*. Uma vez que a vulneração tem acontecido, é importante tomar os passos corretos para remediar as consequências da vulneração. Recomenda-se ter conhecimento e informar o pessoal desses passos antes de uma vulneração. Tão pronto como tiver conhecimento de uma vulneração, assegure-se de:

- **Informar sem demora indevida** ao seu diretor ou supervisor, assim como ao ponto focal de Proteção de Dados, à equipa legal ou a outra pessoa encarregada da proteção de dados da Sociedade Nacional. Se não souber quem é responsável, comunique as preocupações à liderança da sua organização.

Os seguintes passos devem ser realizados em colaboração com estes expertos:

- **Investigar a amplitude de uma vulneração:** Que tipo de vulneração? Que tipo de dados? Quantos dados? Duração da vulneração? Quais pessoas em causa? Exposição dos dados a quem?
- **(em paralelo) Tomar medidas de mitigação** (em função do tipo de vulneração, tais como cortar sistemas de TI, recuperar *backup* de dados, entrar em contato com a pessoa não autorizada para pôr termo a uma exposição de dados, colmatar as lacunas, informar aos sócios envolvidos e potencialmente aos doadores.
- **Avaliar o nível de risco para as pessoas em causa e fazer esforços razoáveis para informar às pessoas em causa se os riscos forem elevados** por motivos de transparência.
- Em função das leis nacionais, **considerar a possibilidade de informar às autoridades de proteção de dados do seu país.**
- **Prepare as informações/lições aprendidas** e **eliminar fraquezas organizativas ou técnicas.**
- **Melhorar o plano de resposta para a próxima incidência** conforme for necessário de acordo com a experiência obtida**.**

Instruções ao Pessoal e aos Voluntários

A primeira medida para uma efetiva proteção de dados é a conscientização. Portanto, é importante informar ao seu pessoal e voluntários dos princípios essenciais de proteção de dados e como abordá-los no ciclo do programa de AMV. Recomenda-se manter sessões regulares de formação sobre proteção de dados, em particular para as pessoas novas na organização como parte da sua incorporação. Os materiais de formação podem ser preparados com antecedência para a incorporação e como reciclagem para aqueles que têm recebido a formação anteriormente. Nessa formação, a

importância da proteção de dados deve ser salientada e os princípios essenciais explicados; e, o mais importante, deve-se explicar quais são as considerações de proteção de dados devem ser abordadas nos processos de AMV e as responsabilidades do pessoal e dos voluntários em função das suas funções. Também deve haver consciência sobre como responder às vulnerações de dados.

Análise e Monitoramento de Riscos de Proteção de Dados

Para conseguir que a proteção de dados seja verdadeiramente salvaguardada da privacidade dos beneficiários nos seus programas, recomenda-se encarecidamente que se anote as considerações de proteção de dados que esteja a implementar. Por quê? Porque ajuda a estabelecer uma abordagem estruturada e consistente para gerir os riscos e achar um bom equilíbrio. Além disso, documentar os riscos e as decisões tomadas será importante no caso de uma auditoria ou investigação seja necessária.

Existem algumas ferramentas que podem ser usadas na análise e documentação de riscos ligados à proteção de dados:

Matriz de Riscos e Registo de Riscos. O *kit* de ferramentas de AMeE abrange a análise de riscos na Análise da Preparação (Módulo M1_1 Preparar e Analisar), a Avaliação (Módulo M2_4), e a Resposta (Módulo M3_1_4); também os riscos adicionais descritos para a programação de Dinheiro em troca de Trabalho e Vouchers. A mesma matriz de riscos e o registo de riscos podem ser usados para garantir que os elementos de proteção de dados sejam revistos junto com os outros tipos de riscos. Uma nova categoria de proteção de dados poderá ser criada para classificar os riscos de forma apropriada. A análise desses riscos e a criação de medidas de mitigação serão importantes. À medida que o programa se desenvolver, os riscos deverão ser revistos e atualizados conforme as necessidades.

Avaliação do Impacto de Proteção de Dados (AIPD).[15] Esta é uma ferramenta formal para documentar as considerações de proteção de dados para os riscos identificados, assim como as medidas de mitigação previstas. A preparação pode requerer uma consulta externa e a inclusão de partes interessadas relevantes, como os seus colegas do departamento. Não é necessária em todos os casos a realização de uma AIPD tão aprofundada, em particular quando se realizam programas de AMV similares. Pode ser necessária quando forem usados novos métodos e tecnologia e os impactos nos beneficiários não forem conhecidos ainda. Também pode ser caso de apoio quando existem preocupações potenciais dos membros da comunidade em termos de tratamento dos seus dados, para determinar onde se encontram os riscos efetivos e se podem ser mitigados.

[15] Para mais detalhes, ver o Manual sobre Proteção de Dados na Ação Humanitária. Além disso, pode-se encontrar um modelo de AIPD na seção de referências desta orientação.

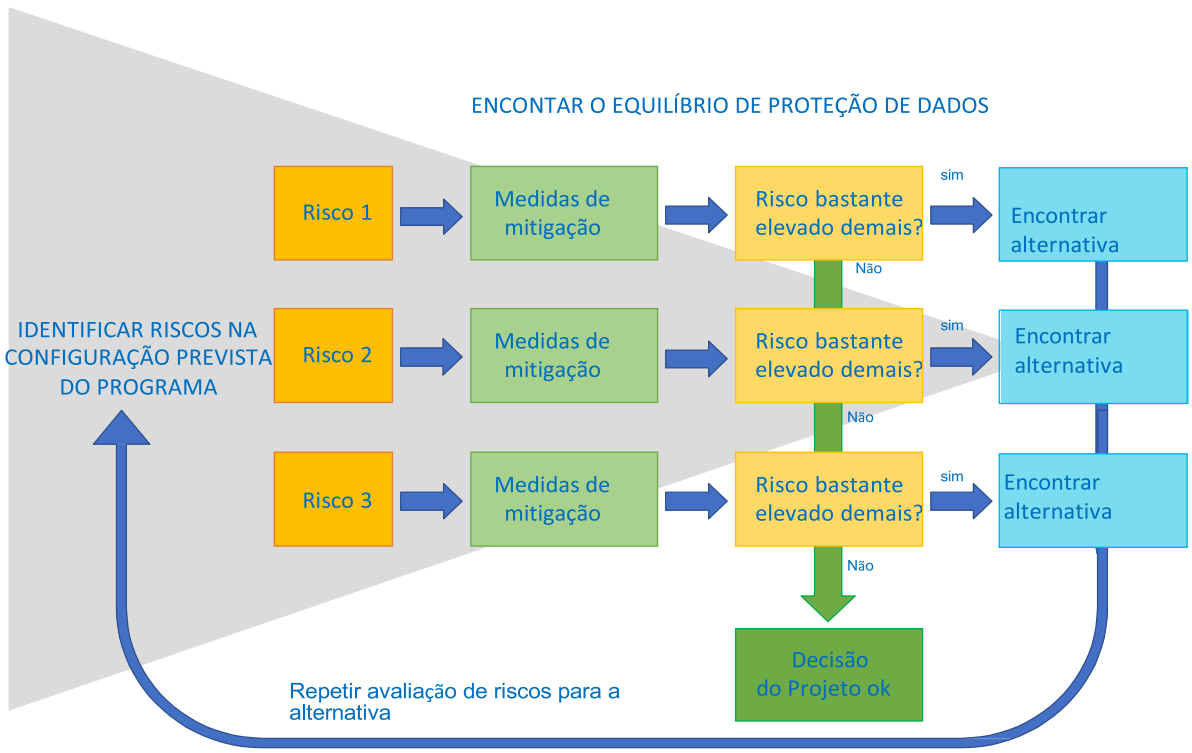

Figura 4: Equilíbrio de riscos e ações ligadas à proteção de dados

A Figura 4 tem por objetivo ajudar refletir sobre a avaliação de riscos de proteção de dados. Isto requer identificar e registar os riscos e as possíveis medidas de mitigação, determinar o nível de riscos (baseado no impacto e na probabilidade) e encontrar alternativas a considerar. Por exemplo:

Inclusão de FSFs?

> Risco 1: Uso de dados para outros efeitos além do acordado;

> Medida de mitigação: deve ser proibido no contrato;

> Risco bastante elevado demais? Sim, porque a reputação e a fiabilidade do FSF são questionáveis;

> Alternativa: outro FSF, dinheiro em envelopes ou em espécie;

> Repetir a avaliação de riscos para a alternativa

Se uma avaliação inicial dos riscos revela que a configuração do programa apresenta elevados riscos de proteção de dados, é aconselhável realizar a avaliação através de um formato formal de AIPD. A obrigação de realizar uma AIPD formal corresponde à organização que lidera o programa, no caso de uma associação para a implementação.

A realização de uma AIPD formal deve ser considerada (e, de acordo com algumas leis de proteção de dados, pode ser requerida), por exemplo, nas situações indicadas abaixo. Note-se: Todas essas formas de tratamento de dados são estritamente sujeitas ao princípio de minimização de dados e de necessidade. A AIPD não pode justificar tratamentos de dados desnecessários.

- Nova tecnologia está a ser usada para recolher, administrar ou conservar dados pessoais (armazenagem na nuvem, geolocalização, mídia social, etc.). Não saber como funcionam as tecnologias modernas pode aumentar o risco de acesso não

autorizada (*hacking*) e abrir as possibilidades à vigilância não autorizada.

- As pessoas podem estar sujeitas a uma tomada de decisões automatizadas ou à realização de perfis. A tomada de decisões automatizadas interfere muito com a proteção de dados, porque as decisões são tomadas além do controlo da pessoa e sem a possibilidade para a pessoa rastrear e discutir a decisão. A realização de perfis é problemática porque a criação de um perfil de pessoas envolve colocar as pessoas em certas categorias sem uma interação prévia real com ela.
- Os dados pessoais podem ser transferidos a um terceiro (ou país terceiro) sem normas de proteção de dados similares. Tal como foi discutido, a partilha de dados pode resultar na perda de controlo sobre como os dados são usados. Só deve ser realizada quando a outra parte tiver uma norma adequada de proteção de dados. Se não for o caso e os dados deverem ser compartilhados de todos modos, é importante avaliar de forma aprofundada se isto seria um risco grande demais para os beneficiários (categoria de dados, norma de proteção, etc.)
- Os dados sensíveis, tais como os dados sobre o estado de saúde, a orientação religiosa ou os dados biométricos, podem ser tratados em grande escala (número de pessoas, variedade dos dados, duração do tratamento, âmbito geográfico, etc.). Esses dados são muito sensíveis, pois correspondem a aspectos muito pessoais e privados da vida de uma pessoa. Além disso, este tipo de informações nas mãos incorretas pode ser muito prejudicial para os beneficiários.
- A vigilância em massa pode ser parte do programa e interfere muito com os direitos de todas as pessoas envolvidas, pois o facto de não estar sujeito a um controlo constante de outros ou de sistemas automatizados é uma parte importante da privacidade.
- Pode acontecer uma consolidação e cruzamento de dados de diferentes fontes. A combinação de vários conjuntos de dados sobre uma pessoa aumenta o risco para a privacidade da pessoa.

Independentemente do formato, a avaliação de riscos deve ser feita antes do início do programa, junto com a avaliação de riscos geral do programa, conforme descrito no *kit* de ferramentas de AMeE.

Se tiver perguntas e preocupações relativas à proteção de dados, não duvide em comunicar com o seu diretor e/o a sua equipe legal. Também pode enviar as suas consultas ao Centro Monetário, que é um recurso para a AMV de todo o Movimento. O Centro Monetário apoia aos profissionais da assistência monetária, oferece materiais, incluindo lições aprendidas de outras Sociedades Nacionais, e pode ter considerado questões similares de outros sócios do Movimento no passado.

Engajamento Comunitário e Responsabilização (ECR)

Tal como foi referido em todos os capítulos, informar aos beneficiários e contar com um serviço de apoio e um mecanismo de *feedback* são aspectos importantes da implementação da proteção de dados. Quando a comunicação com os beneficiários for feita por uma equipa individual de ECR, é importante que seja ciente das considerações de proteção de dados e estiver segura de que tem informação para abordar as questões sobre a proteção de dados ou *know how* para referir aquelas perguntas a alguém que possa esclarecer.

IX. Referências

Políticas e Orientações

- Manual sobre Proteção de Dados na Ação Humanitária do CICV e do Centro de Privacidade de Bruxelas (em inglês)
- Política da FICV sobre Proteção de Dados (em inglês)
- Normas do CICV sobre Proteção de Dados (em inglês)
- Política do CICV sobre o Tratamento de Dados Biométricos (em inglês)
- Política de Segurança da Informação da FICV (em inglês)
- Folheto de Proteção de Dados de Gestão da Informação da FICV (em inglês)

Modelos e material auxiliar

Os materiais que se seguem devem ser contextualizados pelas Sociedades Nacionais para cumprir os requisitos próprios delas; em particular, o cumprimento das suas leis e políticas nacionais de proteção de dados, que podem ser mais estritas do que o padrão de proteção de dados aplicado na preparação desses documentos.

- Modelo de contrato padronizado com Fornecedor de Serviços Financeiros (em inglês)
- Questionário prévio ao contrato com o Fornecedor de Serviços Financeiros /modelo de *due diligence* (em inglês)
- Modelo de AIPD (em inglês)
- Modelo de Mostra de Aviso de Privacidade (em inglês)

X. Agradecimentos

Este documento foi possível graças às seguintes organizações