Principes de protection des données dans le contexte des programmes de transferts monétaires

### 1. Respecter la vie privée

Principe : Les organisations sont tenues de respecter la vie privée des bénéficiaires et de reconnaître que la collecte et le traitement de leurs données personnelles représentent une menace potentielle pour cette dernière.

### 2. Protéger les données personnelles

Principe : Les organisations doivent « protéger » les données personnelles qu’elles collectent auprès des bénéficiaires, soit pour leur propre usage, soit pour une utilisation par des tiers, pour chaque programme de transferts monétaires ou électroniques qu’elles initient ou mettent en œuvre.

### 3. Comprendre les flux de données et les risques

Principe : Les organisations doivent analyser, documenter et comprendre le flux de données relatives aux bénéficiaires pour chaque programme de transferts monétaires ou électroniques qu’elles initient ou mettent en œuvre de manière individuelle ou en collaboration avec d’autres organisations, et élaborer des stratégies d’atténuation des risques qui pourraient s’avérer nécessaires pour traiter tout risque découlant de ces flux.

### 4. Garantir la qualité et l’exactitude des données

Principe : Les organisations doivent veiller à l’exactitude des données personnelles qu’elles collectent, conservent et utilisent, y compris en maintenant des informations à jour, pertinentes et non excessives au regard des finalités pour lesquelles elles sont utilisées, et en ne conservant pas les données plus longtemps que nécessaire.

### 5. Obtenir le consentement des bénéficiaires ou les informer de l’utilisation faite de leurs données

Principe : Au moment de la collecte des données, les bénéficiaires doivent être informés de la nature des données recueillies, des personnes avec lesquelles elles seront partagées et de la personne responsable de l’utilisation sécurisée de leurs données. Elles doivent également avoir la possibilité de contester l’utilisation faite des données et de se retirer du programme si elles ne souhaitent pas que leurs données personnelles soient utilisées aux fins décrites.

### 6. Sécurité

Principe : Les organisations doivent définir des normes de sécurité techniques et opérationnelles appropriées pour chaque étape de la collecte, de la transmission et de l’utilisation des données relatives aux bénéficiaires afin d’empêcher l’accès non autorisé, la divulgation ou la perte de données. En particulier, toutes les menaces externes doivent être identifiées et des mesures doivent être prises pour atténuer les risques qui en découlent.

### 7. Élimination des données

Principe : Les organisations ne doivent pas conserver les données relatives aux bénéficiaires plus longtemps que nécessaire, sauf pour des raisons claires, justifiables et documentées ; dans le cas contraire, les données détenues par l’organisation et les tiers concernés doivent être éliminées.

### 8. Redevabilité

Principe : Les organisations doivent établir des mécanismes par lesquels un bénéficiaire peut demander des informations sur le type de données personnelles qu’une organisation détient à son sujet ainsi que des mécanismes destinés à recevoir toute réclamation ou demande d’information que les bénéficiaires peuvent avoir au sujet de l’utilisation de leurs données personnelles, et à y répondre.

Source : CaLP, *Protéger la vie privée des bénéficiaires : Principes et normes opérationnelles pour une utilisation sécurisée des données personnelles dans les programmes de transferts monétaires et électroniques* (2013).