مبادئ حماية البيانات في مجال برمجة التحويلات النقدية

### 1- الاحترام

المبدأ: تحترم المنظمة خصوصية المستفيدين وتعترف بأن حصولها على معلوماتهم الشخصية قد يهدد خصوصيتهم.

2- ضمان الحماية عبر التصميم

المبدأ: تحرص المنظمة على ضمان الحماية "عبر التصميم" للبيانات التي تستلمها من المستفيدين لكي تيسر عملها أو لتوفيرها لطرف ثالث، وذلك عند كل عملية تحويل.

3- فهم عملية تدفق البيانات والمخاطر المرتبطة بها

المبدأ: تحرص المنظمة على تحليل بيانات المستفيدين وتوثيقها وفهمها عند كل عملية تحويل. وتضع استراتيجية للحد من المخاطر التي قد تواجه تدفق البيانات.

4- الجودة والدقة

المبدأ: تحرص المنظمة علىدقة البينات الشخصية التي تجمعها وتحفظها وتستخدمها، عبر ادخال التحديثات عليها بانتظام، وعدم الاحتفاظ بها لمدة تفوق المدة المطلوبة.

5- الحصول على موافقة المستفيد عند استعمال البيانات الخاصة به.

المبدأ: عند الحصول على المعلومات، يتم ابلاغ المستفيد عن الجهات التي ستحصل عليها والجهات المعنية بحمايتها، كما يعطى الفرصة لطرح الأسئلة حول سبب استعمالها أو حتى الانسحاب من البرنامج إن لم يوافق على ظروف هذا الاستعمال.

6- الأمن

المبدأ: تنفذ المنظمة المعايير الفنية والتشغيلية المناسبة في كل مرحلة من مراحل الجمع، والتحويل، واستخدام البيانات. وذلك من أجل تفادي أي نفاذ غير مسموح به إلى البيانات، أو فقدان أي معلومات. ويتم تحديد التهديدات الخارجية على البيانات وتنفيذ التدابير اللازمة للتصدي لها والحد من المخاطر الناتجة عنها.

7- الاحنفاظ بالبيانات

المبدأ: لا يجوز أن تحتفظ المنظمة بالبيانات لمدة أطول من المدة المطلوبة إلا إذا كان لذلك مبررات موثقة، وفي الظروف الطبيعية، تتلف البيانات بعد مرور المدة المطلوبة.

8- المسائلة

المبدأ: تضع المنظمة آليات تسمح للمستفيد معرفة المعلومات المتعلقة به التي تتوفر لدى المنظمة، وآليات أخرى تسمح للمستفيد بتقديم الشكاوى والتعبير عن مخاوفه إذاء استعمال البيانات الشخصية الخاصة به.

المصدر:

Protecting Beneficiary Privacy: Principles and operational standards for the secure use of   
personal data in cash and e-transfer programmes (2013) CaLP