Principios de protección de datos en PTE

### 1. Respeto

Principio: Las organizaciones deben respetar la privacidad de los beneficiarios y ser conscientes de que la obtención y el procesamiento de los datos personales representa una amenaza potencial para esa privacidad.

### 2. Proteger mediante el diseño

Principio: Las organizaciones deben “proteger mediante el diseño” los datos personales que obtengan de los beneficiarios, ya sea para su propio uso o para el uso por parte de terceros, de todos los programas de transferencia de efectivo o transferencia electrónica que inicien o implementen.

### 3. Comprender los flujos de datos y los riesgos

Principio: Las organizaciones deben analizar, documentar y comprender los flujos de datos de los beneficiarios de todos los programas de transferencia de efectivo o transferencia electrónica que inicien o implementen, dentro de sus propias organizaciones y entre sus organizaciones y terceros, y desarrollar estrategias de mitigación de riesgos que pudieran ser necesarias para hacer frente a los riesgos derivados de estos flujos.

### 4. Calidad y exactitud

Principio: Las organizaciones deben garantizar la exactitud de los datos personales que recopilan, almacenan y utilizan, manteniendo la información al día, pertinente y no excesiva en relación con los fines para los que se procesan, y no manteniendo los datos durante más tiempo del necesario.

### 5. Obtener el consentimiento o informar a los beneficiarios sobre el uso de sus datos

Principio: En el momento de la recogida de datos, los beneficiarios deben ser informados acerca de la naturaleza de los datos que se recogen, con quién se van a compartir y quién es responsable de su buen uso, y darle la oportunidad de hacer preguntas sobre el uso que se hará de sus datos y de retirarse del programa en caso de que no desee que sus datos personales se utilicen para los fines descritos.

### 6. Seguridad

Principio: Las organizaciones deben aplicar las normas de seguridad técnicas y operativas adecuadas en cada etapa de la recogida, transferencia y uso de los datos de los beneficiarios para evitar el acceso no autorizado, su difusión o extravío, y cualquier amenaza externa debe ser identificada y se han de adoptar las medidas oportunas para mitigar los riesgos derivados.

### 7. Destrucción

Principio: Las organizaciones no deben mantener los datos de los beneficiarios por más tiempo del necesario a menos que tengan razones claras, justificadas y documentadas para hacerlo; de lo contrario, los datos en poder de la organización y de terceros deben ser destruidos.

### 8. Rendición de cuentas

Principio: Las organizaciones deben establecer mecanismos mediante los cuales el beneficiario pueda solicitar información sobre cuál es la información que la organización posee sobre ellos y mecanismos para recibir y responder a las quejas o inquietudes de los beneficiarios sobre el uso de sus datos personales.

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