Принципы защиты данных ПДП

### 1.Уважение

Принцип: Организации должны уважать частную жизнь бенефициаров и признавать, что получение и обработка их персональных данных может представлять угрозу сохранению тайны частной жизни.

### 2.Преднамеренная защита

Принцип: Организации должны «преднамеренно защищать» личные данные, которые они получают от бенефициаров для собственного использования либо для использования третьими сторонами, для каждой программы с использованием наличных денег или электронных переводов, которую они инициируют или проводят.

### 3.Понимание процесса передачи данных и рисков

Принцип: Организации должны анализировать, документировать и понимать, как организовано передвижение данных бенефициаров в каждой программе с использованием наличных денег или электронных переводов, которую они инициируют или проводят силами своих организаций или совместно силами своих и других организаций, а также разрабатывать стратегии снижения рисков, которые могут потребоваться для работы с любыми рисками, возникающими при передаче данных.

### 4.Качество и достоверность

Принцип: Организации должны гарантировать достоверность личных данных, которые они собирают, хранят и используют, в том числе путём обновления информации, а также обеспечивая актуальность и исключая избыточность информации в отношении цели, с которой производится обработка информации, а также не хранить данные дольше, чем это необходимо.

### 5.Получение согласия бенефициаров на использование их данных

Принцип: В момент получения данных следует информировать бенефициаров о том, какие данные собираются, кому они будут предоставлены, а также кто отвечает за безопасность использования их данных. Бенефициарам должна быть предоставлена возможность усомниться в том, как будут использованы их данные, и покинуть программу, если они не захотят, чтобы их данные были использованы с указанной целью.

### 6.Безопасность

Принцип: Организации должны внедрять соответствующие стандарты технической и оперативной безопасности для каждой стадии сбора, передачи и использования данных бенефициаров, чтобы предотвратить несанкционированный доступ, разглашение или утрату данных, и, в особенности, следует идентифицировать все внешние угрозы и принять меры к снижению уровня возникающих рисков.

### 7.Ликвидация

Принцип: Организации не должны хранить данные бенефициаров дольше, чем требуется, кроме случаев, когда у них есть для этого ясные, обоснованные и документированные причины; в противном случае данные, хранящиеся у организации и любых соответствующих третьих сторон, должны быть уничтожены.

### 8.Отчётность

Принцип: Организации должны внедрить механизмы, согласно которым бенефициар может запросить информацию о том, какие его личные данные имеются у организации, а также механизмы для получения любых жалоб и выражений беспокойства, которые бенефициары могут иметь относительно использования их личных данных, а также реагирования на них.

Источник: Защита конфиденциальности бенефициаров: Принципы и оперативные стандарты безопасного использования личных данных в программах выплаты наличных денег и электронных переводов / Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes (2013) CaLP