# **ПОЛОЖЕНИЕ О ВНУТРЕННЕМ КОНТРОЛЕ ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ**

Настоящее Положение разработано в соответствии с:

* **Законом Республики Беларусь «О защите персональных данных»**,
* **Техническими нормативными правовыми актами в области защиты информации**,
* **Рекомендациями контролирующих органов по обеспечению безопасности персональных данных**,
* Актуальными локальными нормативными правовыми актами (ЛНПА) **[Наименование организации]**, регулирующими вопросы защиты информации и внутреннего контроля.

### **1.1. Цель и задачи**

Целью настоящего Положения является установление системы внутреннего контроля за обработкой персональных данных в **[Наименование организации]** (далее – Общество), направленной на:

* обеспечение соблюдения требований законодательства;
* защиту прав субъектов персональных данных;
* предотвращение неправомерного использования персональных данных;
* минимизацию рисков, связанных с обработкой и хранением персональных данных;
* организацию внутреннего контроля и мониторинга выполнения требований по защите персональных данных.

### **1.2. Объект внутреннего контроля**

Объектами внутреннего контроля являются:

* процессы обработки персональных данных, включая их сбор, хранение, передачу и уничтожение;
* системы и технологии, используемые для обработки и защиты персональных данных;
* процедуры разграничения доступа к персональным данным;
* меры криптографической и технической защиты данных;
* действия сотрудников, имеющих доступ к персональным данным.

### **ГЛАВА 2. ОРГАНИЗАЦИЯ ВНУТРЕННЕГО КОНТРОЛЯ**

**2.1. Основные направления внутреннего контроля**

Внутренний контроль за обработкой персональных данных включает следующие ключевые направления:

1. **Соблюдение законодательства** – мониторинг выполнения требований Закона «О защите персональных данных», оценка соответствия внутренних процессов действующим нормативным актам.
2. **Разграничение доступа** – контроль прав доступа к информационным системам с персональными данными, ограничение по принципу необходимости.
3. **Техническая и криптографическая защита** – контроль мер защиты данных от несанкционированного доступа, применение сертифицированных средств защиты.
4. **Мониторинг и аудит** – регулярные проверки соблюдения требований по обработке персональных данных, анализ выявленных нарушений.
5. **Обучение сотрудников** – повышение осведомленности и компетенции персонала по вопросам защиты данных.

**2.2. Виды внутреннего контроля**

Внутренний контроль осуществляется в трех формах:

* **Предварительный** – проверка соответствия процедур обработки персональных данных требованиям законодательства до их внедрения.
* **Текущий** – мониторинг соблюдения требований в процессе обработки данных.
* **Последующий** – аудит результатов обработки, выявление несоответствий и принятие корректирующих мер.

### **ГЛАВА 3. СТРУКТУРА И ПОЛНОМОЧИЯ СУБЪЕКТОВ КОНТРОЛЯ**

**3.1. Ответственный за внутренний контроль за обработкой персональных данных**

На ответственного за внутренний контроль возлагаются следующие обязанности:

* контроль выполнения требований законодательства и локальных нормативных актов;
* организация мониторинга процессов обработки персональных данных;
* проведение аудита по защите персональных данных;
* взаимодействие с контролирующими органами по вопросам внутреннего контроля и защиты данных;
* инициирование корректирующих мероприятий при выявлении нарушений.

**3.2. Руководители подразделений**

Руководители подразделений обязаны:

* обеспечивать выполнение требований по защите персональных данных в своем подразделении;
* контролировать корректность обработки данных сотрудниками;
* взаимодействовать с ответственным за защиту персональных данных по вопросам контроля.

**3.3. Сотрудники, работающие с персональными данными**

Обязанности сотрудников:

* соблюдать требования законодательства и внутренних регламентов;
* обеспечивать защиту данных в рамках своей деятельности;
* информировать руководство о выявленных нарушениях.

### **ГЛАВА 4. ПРОЦЕДУРЫ КОНТРОЛЯ И МОНИТОРИНГА**

**4.1. Организация проверок**

Мониторинг обработки персональных данных осуществляется через следующие процедуры:

* **Анализ соответствия процессов обработки требованиям законодательства**;
* **Проверка полноты, достоверности и актуальности персональных данных**;
* **Оценка соблюдения правил доступа к данным**;
* **Аудит мер технической и криптографической защиты**;
* **Контроль регистрации и обработки запросов субъектов персональных данных**.

**4.2. Проведение аудитов**

Аудит включает:

* **Проверку выполнения требований по хранению и уничтожению персональных данных**;
* **Анализ случаев нарушения конфиденциальности и их последствий**;
* **Мониторинг технических средств защиты данных**;
* **Анализ отчетности по обработке персональных данных**.

### **ГЛАВА 5. МЕРЫ РЕАГИРОВАНИЯ НА ВЫЯВЛЕННЫЕ НАРУШЕНИЯ**

**5.1. Виды нарушений**

Нарушения, подлежащие внутреннему контролю:

* некорректное оформление согласия субъекта персональных данных;
* неправомерная передача персональных данных третьим лицам;
* отсутствие должных мер защиты информации;
* нарушение сроков хранения персональных данных.

**5.2. Ответственность за нарушения**

При выявлении нарушений могут применяться:

* **дисциплинарные меры** – предупреждение, выговор, лишение премии;
* **административные меры** – наложение штрафов;
* **корректирующие меры** – исправление недочетов, усиление процедур безопасности.

### **ГЛАВА 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

**6.1. Ознакомление сотрудников** Все сотрудники **[Наименование организации]** обязаны ознакомиться с данным Положением и соблюдать установленные требования.

**6.2. Пересмотр и обновление** Положение подлежит пересмотру при изменении законодательства или внутренних процессов обработки персональных данных.

**6.3. Вступление в силу** Настоящее Положение вступает в силу с момента его утверждения.