УТВЕРЖДЕНЫ
приказом № _____
от «___» _____ 20__ г.

ПРАВИЛА
осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите персональных данных,
установленным Федеральным законом «О персональных данных», принятыми
в соответствии с ним нормативными правовыми актами и локальными актами

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами (далее – Правила) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в _____ _____(далее – Учреждение).

1.2 Настоящие Правила разработаны в соответствии с Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.3 Внутренний контроль состояния защиты информации включает в себя:

контроль организации защиты информации;

контроль эффективности защиты информации.

2. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

2.1 В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организовывается проведение периодических проверок условий обработки персональных данных.

2.2 Проверки осуществляются ответственным за организацию обработки персональных данных, либо комиссией, созданной на основании приказа руководителя.

2.3 В проведении проверки не может участвовать сотрудник, прямо или косвенно заинтересованный в её результатах.

2.4 Проверка соответствия обработки персональных данных установленным требованиям проводится не реже одного раза в год на основании утвержденного руководителем «Плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям» или на основании письменного заявления о нарушении правил обработки.

2.5 Проведение внеплановой проверки организуется в течение 3 рабочих дней с момента поступления соответствующего заявления.

2.6 При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям полностью, объективно и всесторонне производится проверка:

соблюдения принципов обработки персональных данных;

соответствия локальных актов в области персональных данных действующему законодательству Российской Федерации;

выполнения сотрудниками требований и правил обработки персональных данных;

актуальности информации о законности целей обработки персональных данных и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований обработки и обеспечения безопасности персональных данных;

правильности осуществления сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных;

актуальности перечня лиц, имеющих доступ к персональным данным;

соблюдения прав субъектов персональных данных;

порядка взаимодействия с субъектами персональных данных, в том числе соблюдения сроков, требований по уведомлениям, порядка разъяснения субъектам необходимой информации, порядка реагирования на запросы субъектов персональных данных, порядка действий при достижении целей обработки и отзыве согласия субъекта персональных данных, наличия необходимых согласий субъектов персональных данных;

актуальности сведений, содержащихся в уведомлении об обработке персональных данных;

актуальности перечня информационных системах персональных данных персональных данных персональных данных;

знания и соблюдения сотрудниками положений действующего законодательства Российской Федерации в области персональных данных, локальных актов Учреждения;

соблюдения условий сотрудниками конфиденциальности персональных данных;

соблюдения сотрудниками требований по обеспечению безопасности персональных данных;

наличия и актуальности локальных актов, технической и эксплуатационной документации, технических и программных средств информационной системы персональных данных персональных данных персональных данных.

2.7 Контроль осуществляется непосредственно на месте обработки персональных данных путем опроса сотрудников и осмотра рабочих мест, участвующих в процессе обработки персональных данных.

2.8 По результатам проведения внутреннего контроля составляется протокол проведения проверки.

2.9 При выявлении нарушений в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

2.10 О результатах проведения проверки и мерах, необходимых для устранения нарушений, руководителю Учреждения докладывает ответственный за организацию обработки персональных данных.

ПРИЛОЖЕНИЕ 1

П Р О Т О К О Л
проведения внутренней проверки соответствия обработки персональных данных требованиям к защите персональных данных

«___» _____ 20__ г. г. Белгород № _____

Комиссия в составе:
председатель комиссии

_____
(Ф.И.О., должность)

члены комиссии

_____
(Ф.И.О., должность)

_____
(Ф.И.О., должность)

провела проверку соответствия обработки персональных данных требованиям к защите персональных данных.

Проверка проводилась в соответствии с «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами».

Выявленные нарушения:

_____
_____

Меры по устранению нарушений:

_____
_____

Срок устранения нарушений: _____

Председатель комиссии:

_____ _____ _____
Должность Ф.И.О.

Члены комиссии:

_____ _____ _____
Должность Ф.И.О.

_____ _____ _____
Должность Ф.И.О