УТВЕРЖДАЮ
Директор ОГБУ «УСЗСОН
по Казачинско-Ленскому району»
_____ К.Г.Широбокова
«02» сентября 2022 г.

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (далее - Правила), разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и определяют порядок и мероприятия, проводимые в рамках внутреннего контроля соответствия обработки персональных данных (далее - внутренний контроль) в ОГБУ «УСЗСОН по Казачинско-Ленскому району» (далее - Управление).

1.2. Внутренний контроль состоит из перечня мероприятий (внутренних проверок), выполнение которых позволяет оценить соответствие обработки персональных данных в Управлении требованиям Федерального закона «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, Политике в отношении обработки персональных данных в ОГБУ «УСЗСОН по Казачинско-Ленскому району» и иным локальным актам Управления, а также своевременно выявить и предотвратить нарушения законодательства Российской Федерации в сфере персональных данных.

1.3. В целях организации и осуществления внутреннего контроля в Управлении создается комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных в Управлении требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (далее - Комиссия). Численный и персональный состав Комиссии утверждается приказом Управления.

1.4. Внутренний контроль проводится не реже одного раза в год.

1.5. Настоящие Правила подлежат анализу и, при необходимости, пересмотру в случаях изменения законодательства Российской Федерации в отношении обработки персональных данных.

2. ФОРМИРОВАНИЕ ПЛАНА ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Проверки, осуществляемые в рамках внутреннего контроля, могут быть плановыми и внеплановыми.

2.2. Плановые проверки соответствия обработки персональных данных установленным

требованиям проводятся на основании подготовленного Комиссией ежегодного плана проведения внутренних проверок режима обработки и защиты персональных данных в Управлении (далее - План проведения внутренних проверок).

2.3. План проведения внутренних проверок должен содержать следующую информацию:

- наименование мероприятий (внутренних проверок);
- периодичность мероприятий (внутренних проверок);
- планируемые даты мероприятий (внутренних проверок);
- перечень лиц, ответственных за проведение мероприятий (внутренних проверок).

2.4. Ежегодный план проведения внутренних проверок утверждается локальным актом Управления.

2.5. В проведении мероприятий внутреннего контроля не могут участвовать сотрудники Управления, прямо или косвенно заинтересованные в их результатах.

3. ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВЫХ ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ

3.1. Внутренние проверки проводятся лицами, ответственными за проведение контрольных мероприятий согласно Плану проведения внутренних проверок, с привлечением при необходимости иных сотрудников Управления (в пределах их компетенции).

3.2. Внутренние проверки проводятся при непосредственном участии сотрудники Управления, осуществляющих обработку персональных данных.

3.3. Контроль соответствия условий обработки персональных данных осуществляется непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников Управления, участвующих в процессе обработки персональных данных.

3.4. При проведении внутреннего контроля должны быть установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- соблюдение мер по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- порядок и условия применения средств защиты информации;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- осуществление мероприятий по обеспечению целостности персональных данных;

- соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки персональных данных;

- наличие правовых оснований по сбору копий документов, содержащих персональные данные.

3.5. По результатам проведения внутренней проверки лицом, ответственным за проведение мероприятия согласно Плану проведения внутренних проверок, оформляется Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в Управлении (далее - Отчет о результатах проведения внутренней проверки). Форма Отчета о результатах проведения внутренней проверки приведена в ПРИЛОЖЕНИИ № 1 к настоящим Правилам.

3.6. В случае выявления нарушений соответствия обработки персональных данных установленным требованиям сведения о выявленных нарушениях фиксируются в Отчете о результатах проведения внутренней проверки.

3.7. Отчет о результатах проведения внутренней проверки предоставляется Комиссии лицом, ответственным за проведение мероприятия согласно Плану проведения внутренних проверок.

3.8. Для устранения нарушений, выявленных по результатам внутренних проверок, Комиссия формирует План мероприятий по устранению нарушений, выявленных в результате проведения внутренней проверки режима обработки и защиты персональных данных в Управлении (далее - План мероприятий по устранению нарушений). Форма Плана мероприятий по устранению нарушений приведена в ПРИЛОЖЕНИИ № 2 к настоящим Правилам.

3.9. Комиссия определяет срок устранения каждого нарушения, выявленного в процессе проведения внутренней проверки.

3.10. По результатам определения мероприятий, необходимых для устранения выявленных нарушений, и сроков их выполнения, лица, причастные к выявленному нарушению, приступают к их устранению.

3.11. По результатам проведения мероприятий, включенных в ежегодный План проведения внутренних проверок, Комиссия ежегодно или по запросу руководителя Управления формирует Отчет о выполнении плана проведения, внутренних проверок режима обработки и защиты персональных данных в Управлении (далее - Отчет о выполнении плана проведения внутренних проверок). Форма Отчета о выполнении плана проведения внутренних проверок приведена в ПРИЛОЖЕНИИ № 3 к настоящим Правилам.

3.12. Отчет по результатам внутреннего контроля Комиссия направляет руководителю Управления.

3.13. При необходимости в Управлении дополнительно может вестись Журнал проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства, а также локальным актам Управления (далее - Журнал проведения внутреннего контроля). Форма Журнала проведения внутреннего контроля приведена в ПРИЛОЖЕНИИ № 4 к настоящим Правилам.

3.14. Ответственность за своевременное ведение Журнала проведения внутреннего контроля возлагается на Комиссию.

4. ПОРЯДОК ПРОВЕДЕНИЯ ВНЕПЛАНОВЫХ ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Внеплановые проверки соответствия обработки персональных данных установленным требованиям проводятся на основании поступившей информации о нарушении правил обработки персональных данных в Управлении. Проведение внеплановой проверки организуется Комиссией в течение трех рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

4.2. По результатам проведения внеплановой проверки также составляется Отчет о результатах проведения внутренней проверки.

5. ОТВЕТСТВЕННОСТЬ

5.1. Члены Комиссии и лица, ответственные за проведение мероприятий согласно Плану проведения внутренних проверок, обеспечивают конфиденциальность персональных данных, ставших известными им в ходе мероприятий внутреннего контроля.

5.2. Члены Комиссии и лица, ответственные за проведение мероприятий согласно Плану проведения внутренних проверок, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящих Правил.

ПРИЛОЖЕНИЕ № 1 к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами
от « 2 » сентября 2022 г.

Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в ОГБУ «УСЗСОН по Казачинско-Ленскому району»

1. Внутренняя проверка проведена на основании приказа «Об утверждении плана внутренних проверок режима обработки и защиты персональных данных в Управлении от «____»_____20_____г.

2. Проверка проводилась «_____ » 20___ г. по адресу:

3. В ходе проверки было проведено следующее мероприятие:

4. Результат проведения мероприятия: _

____ (дата) _____ (подпись) _____ (расшифровка подписи)

Лица, ответственные за проведение мероприятий (внутренних проверок):

ПРИЛОЖЕНИЕ № 2 к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии *с* ним нормативными правовыми актами от « 2 » сентября 2022 г.

План мероприятий по устранению нарушений, выявленных в результате проведения внутренней проверки режима обработки и защиты персональных данных в ОГБУ «УСЗСОН по Казачинско-Ленскому району»

№ п/п	Мероприятие по устранению нарушений	Мероприятие, при выполнении которого выявлены нарушения	Запланированная дата проведения

ПРИЛОЖЕНИЕ № 3 к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами от « 2 » сентября 2022 г.

Отчет о выполнении плана проведения внутренних проверок режима обработки и защиты персональных данных в ОГБУ «УСЗСОН по Казачинско-Ленскому району»

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» комиссией по осуществлению внутреннего контроля соответствия обработки персональных данных в Управлении требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (далее - Комиссия) было организовано проведение мероприятий (внутренних проверок), выполнение которых позволяет оценить соответствие обработки персональных данных в Управлении (далее - Управление) требованиям Федерального закона «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, Политике в отношении обработки персональных данных в Управлении и иным локальным актам Управления, а также своевременно выявить и предотвратить нарушения законодательства Российской Федерации в сфере персональных данных.

Мероприятия проводились в соответствии с планом проведения внутренних проверок режима обработки и защиты персональных данных в Управлении, утвержденным приказом «Об утверждении плана внутренних проверок режима обработки и защиты персональных данных в ОГБУ «УСЗСОН по Казачинско-Ленскому району» от «_____» 20 г.

Результаты проведения контрольных мероприятий согласно утвержденному плану представлены в таблице №1.

Председатель Комиссии:

(дата) (подпись) _____ (расшифровка подписи)

Заместитель председателя Комиссии:

(дата) (подпись) (расшифровка подписи)

Секретарь Комиссии:

(дата) (подпись) (расшифровка подписи)

Члены Комиссии:

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Таблица №1 - Результаты проведения контрольных мероприятий согласно утвержденному плану

№ п/п	Наименование мероприятия	Периодичность	Планируемая дата	Фактическая дата	Исполнитель	Результат проверки	Мероприятия по устранению нарушений *(заполняется в случае выявления нарушений)*

ПРИЛОЖЕНИЕ № 4 к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами от « 2 » сентября 2022 г.

Журнал проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства, а также локальным актам Управления

№	Мероприятие	Дата проведения	Краткий результат	Отметка об устранении нарушений *(заполняется в случае выявления нарушений)*	ФИО и подпись сотрудника, сделавшего запись