РОССИЙСКАЯ ФЕДЕРАЦИЯ

АДМИНИСТРАЦИЯ МАЛОКАМАЛИНСКОГО СЕЛЬСОВЕТА

РЫБИНСКОГО РАЙОНА КРАСНОЯРСКОГО КРАЯ

РАСПОРЯЖЕНИЕ

 16.07.2025 с. Малая Камала № 48-о

Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты

В целях выполнения требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказа федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», Постановления Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации в администрации Малокамалинского сельсовета Рыбинского района Красноярского края

РАСПОРЯЖАЮСЬ:

1. Утвердить Правила обработки персональных данных в администрации Малокамалинского сельсовета:
	1. Утвердить **Правила** осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных **согласно приложению 1.**
	2. Утвердить Правила работы с обезличенными персональными данными в администрации Малокамалинского сельсовета Рыбинского района Красноярского края согласно приложению 2.
	3. Утвердить Должностную инструкцию лица, ответственного за организацию обработки персональных данных в администрации Малокамалинского сельсовета Рыбинского района согласно приложению 3.
	4. Утвердить Перечень лиц, допущенных к обработке персональных данных в информационной системе персональных данных администрации Малокамалинского сельсовета согласно приложению 4.
	5. Утвердить **Перечень** персональных данных, обрабатываемых в администрации Малокамалинского сельсовета Рыбинского района в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций согласно приложению 5.
	6. Утвердить **Перечень** должностей в администрации Малокамалинского сельсовета Рыбинского района, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных согласно приложению 6.
	7. Утвердить П**еречень** должностей в администрации Малокамалинского сельсовета Рыбинского района, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению 7.
	8. Утвердить **Форму обязательства** о неразглашении информации, содержащей персональные данные согласно приложению 8.
	9. Утвердить Порядок доступа муниципальных служащих и других работников администрации Малокамалинского сельсовета в помещения, в которых ведется обработка персональных данных согласно приложению 9.
	10. Утвердить Типовую форму согласия на обработку персональных данных служащих, иных субъектов персональных данных, а также типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в администрацию Малокамалинского сельсовета согласно приложению 10.
	11. Утвердить Инструкцию пользователя при обработке персональных данных на объектах вычислительной техники согласно приложению 11.
	12. Утвердить **Правила** рассмотрения запросов субъектов персональных данных или их представителей в администрации Малокамалинского сельсовета Рыбинского района согласно приложению 12.
	13. Утвердить Инструкциюпо организации антивирусной защиты в информационных системах персональных данных администрации Малокамалинского сельсовета Рыбинского района согласно приложению 13.
	14. Утвердить Порядок учета, хранения и уничтожения носителей персональных данных в администрации Малокамалинского сельсовета Рыбинского района согласно приложению 14.
	15. Утвердить Порядок реагирования на инциденты информационной безопасности в администрации Малокамалинского сельсовета Рыбинского района согласно приложению 15.
	16. Утвердить Журнал ознакомления работников с локальными нормативными актами в области обработки персональных данных согласно приложению 16.

2. Специалисту 1 категории Малокамалинского сельсовета ознакомить работников администрации Малокамалинского сельсовета с локально правовыми актами под роспись.

1. Контроль за выполнением распоряжения оставляю за собой.
2. Распоряжение вступает в силу после подписания.
3. Опубликовать на официальном сайте органа местного самоуправления в течение 10 дней после утверждения.

Глава сельсовета Н.В. Прохорова

Приложение № 1

к распоряжению

от 16.07.2025 № 48-о

**ПРАВИЛА**

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Цель внутреннего контроля.
2. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных осуществляется с целью проверки соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом №152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами администрации Малокамалинского сельсовета Рыбинского района .

Статья 2. Виды и периодичность внутреннего контроля.

1. Внутренний контроль соответствия обработки персональных данных делится на текущий и периодический.
2. Текущий внутренний контроль осуществляется на постоянной основе Ответственным за обеспечение безопасности персональных данных.
3. Периодический внутренний контроль осуществляется комиссией в соответствии с поручением главы Малокамалинского сельсовета Рыбинского района .

Периодичность проверки – **не реже одного раза в год**.

Статья 3. Порядок создания комиссии для осуществления внутреннего контроля.

1. Проверки осуществляются комиссией, созданной распоряжением главы администрации Малокамалинского сельсовета Рыбинского района, из числа сотрудников администрации Малокамалинского сельсовета Рыбинского района, допущенных к обработке персональных данных, так же возможно привлечение в качестве членов комиссий экспертов.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

1. Проверки осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

Статья 4. Порядок проведения внутренней проверки.

1. При проведении внутренней проверки комиссией должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных;

- состояние учёта бумажных и машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

1. Осуществление внутреннего контроля мероприятий проводятся комиссией периодически в соответствии с Перечнем мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных. Форма Перечня мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных приведена в Приложении 1 к настоящим Правилам.

Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 2 к настоящим Правилам.

1. При выявлении в ходе проверки нарушений в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
2. Протоколы хранятся у председателя комиссии в течение текущего года. Уничтожение Протоколов проводится комиссией самостоятельно по истечении срока хранения.
3. О результатах проверки и мерах, необходимых для устранения нарушений председатель комиссии докладывает главе Малокамалинского сельсовета Рыбинского района .
4. Срок проведения проверки не может составлять более 30 (тридцати) дней со дня принятия решения о её проведении.

Приложение 1

**Перечень**

мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных

|  |  |
| --- | --- |
| № п/п | Краткое описание мероприятий |
| 1 | Контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны |
| 2 | Проверка выполнения требований по условиям размещения автоматизированных рабочих мест (далее - АРМ) в помещениях, в которых размещены средства информационных систем персональных данных (далее - ИСПДн) |
| 3 | Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, разрешенных для обработки персональных данных |
| 4 | Проверка режима допуска в помещения, где размещены средства ИСПДн и осуществляется обработка персональных данных |
| 5 | Проверка соответствия реального уровня полномочий по доступу к персональным данным различных пользователей, установленному в списке лиц, допущенных к обработке персональных данных, уровню полномочий |
| 6 | Проверка наличия и соответствия средств защиты информации в соответствии с указанными в техническом паспорте на ИСПДн |
| 7 | Проверка правильности применения средств защиты информации |
| 8 | Проверка неизменности настроенных параметров антивирусной защиты на рабочих станциях пользователей |
| 9 | Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн |
| 10 | Проверка соблюдения правил парольной защиты |
| 11 | Проверка работоспособности системы резервного копирования |
| 12 | Проведение мероприятий по проверке организации учета и условий хранения съемных носителей персональных данных |
| 13 | Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети "Интернет" |
| 14 | Проверка знаний работниками руководящих документов, технологических инструкций, предписаний, актов, заключений и уровня овладения работниками технологией безопасной обработки информации, изложенных в инструкциях |
| 15 | Проверка знаний инструкций по обеспечению безопасности информации пользователями ИСПДн |
| 16 | Проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки персональных данных и применения средств защиты (сертификатов соответствия и других документов) |

Приложение 2

**Протокол**

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящий Протокол составлен в том, что \_\_.\_\_.202\_ комиссией по внутреннему контролю проведена проверка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

место проверки

Проверка осуществлялась в соответствии с требованиями \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

название документа

В ходе проверки проверено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Председатель комиссии                                          \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия

Члены комиссии:

Должность                                                                \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия

Должность                                                                \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия

Приложение № 2

к распоряжению

от 16.07.2025 № 48-о

**Правила работы**

**с обезличенными персональными данными в администрации** Малокамалинского сельсовета Рыбинского района Красноярского края

**1. Общие положения**

Настоящие Правила работы с обезличенными персональными данными в администрации Малокамалинского сельсовета Рыбинского района Красноярского края (далее – Правила) разработаны с учетом требований Федерального закона от 27.07.2006 № 152‑ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 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».

**2. Условия обезличивания**

Обезличивание персональных данных (далее – ПДн) проводится с целью снижения ущерба от разглашения защищаемых ПДн и снижения требований к защите информационной системы персональных данных (далее – ИСПДн).

Обезличивание персональных данных также осуществляется по достижению целей обработки ПДн или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

Способы обезличивания при условии дальнейшей обработки ПДн:

уменьшение перечня обрабатываемых сведений;

замена части сведений идентификаторами;

замена численных значений минимальным, средним или максимальным значением;

деление сведений на части и обработка их в разных информационных системах и другие способы.

Для обезличивания ПДн применяются любые способы явно не запрещенные законодательно.

Руководители подразделений администрации Двуреченского сельсовета Рыбинского района Красноярского края, непосредственно осуществляющих обработку ПДн, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и определяют способ обезличивания.

**3. Порядок работы с обезличенными персональными данными**

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

парольной политики;

антивирусной политики;

правил работы со съемными носителями;

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

Приложение № 3

к распоряжению

от 16.07.2025 № 48-о

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

лица, ответственного за организацию обработки персональных данных

в администрации Малокамалинского сельсовета Рыбинского района

1. Общие положения

1.1. Настоящая должностная инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных в администрации Малокамалинского сельсовета Рыбинского района (далее - ответственный за организацию обработки персональных данных).

1.2. Ответственный за организацию обработки персональных данных назначается распоряжением Главы Малокамалинского сельсовета.

1.3. Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», нормативными правовыми актами администрации Малокамалинского сельсовета*,* настоящей должностной инструкцией.

2. Должностные обязанности

2.1. Предоставляет субъекту персональных данных по его просьбе информацию.

2.2. Осуществляет внутренний контроль за соблюдением требований законодательства Российской Федерации при обработке персональных данных в администрации Малокамалинского сельсовета Рыбинского района, в том числе требований к защите персональных данных.

2.3. Доводит до сведения работников администрации Малокамалинского сельсовета Рыбинского района положения законодательства Российской Федерации о персональных данных, локальных нормативных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.4. Организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

2.5. Разъясняет субъекту персональных данных юридические последствия отказа предоставления его персональных данных.

3. Права

Для выполнения возложенных задач и функций ответственный за организацию обработки персональных данных наделяется следующими правами:

3.1. Требовать от всех пользователей информационных систем персональных данных выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Участвовать в разработке мероприятий по совершенствованию безопасности персональных данных.

3.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемых персональных данных и технических средств из состава информационных систем.

3.4. Обращаться к главе Малокамалинского сельсовета с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

3.5. Давать свои предложения по совершенствованию организационных, технологических и технических мер защиты персональных данных в администрации Малокамалинского сельсовета Рыбинского района.

1. Ответственность
	1. Ответственный за организацию обработки персональных данных, виновный в нарушении требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» несет ответственность, предусмотренную законодательством Российской Федерации.

 С инструкцией ознакомлен (а):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 дата подпись Ф.И.О.

Приложение 4

к постановлению

от 16.07.2025 № 48-о

ПЕРЕЧЕНЬ

лиц, допущенных к обработке персональных данных в информационной системе персональных данных администрации Малокамалинского сельсовета

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Должность  | Ф.И.О.  | Перечень информационных систем |
| 1 | Глава Малокамалинского сельсовета | Прохорова Н.В. | ФНС России «Личный кабинет налогоплательщика юридического лица»; Енисей СЭД; Регистр МО; Личный кабинет Государственных услуг; Единый портал государственных и муниципальных услуг; официальный сайт администрации Малокамалинского сельсовета; электронная почта администрации Малокамалинского сельсовета; Информационная система ресурс ССТУ. РФ; |
| 2 | Бухгалтер | Белянина Е.И. | СБИС электронная отчетность, Портал СУФД Тензор |
| 3 | Специалист первой категории | Перминова Е.Д. | Енисей СЭД; Регистр МО; Личный кабинет Государственных услуг; ГИС ГМП; ФИАС; Личный кабинет Государственных услуг; ГМИС; официальный сайт администрации Малокамалинского сельсовета; электронная почта администрации Малокамалинского сельсовета; СБИС - электронная отчетность. |
|  |  |  |  |

Приложение № 5

к распоряжению

от 16.07.2025 № 48-о

**Перечень**

персональных данных, обрабатываемых в администрации Малокамалинского сельсовета Рыбинского района в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций

Перечень персональных данных, обрабатываемых в администрации Малокамалинского сельсовета Рыбинского района в связи с реализацией трудовых отношений:

* Фамилия, имя, отчество;
* Место, год и дата рождения;
* Адрес регистрации;
* Адрес проживания (реальный);
* Телефонный номер (домашний, рабочий, мобильный);
* адрес электронной почты;
* Паспортные данные (серия, номер, кем и когда выдан);
* Семейное положение и состав семьи (муж/жена, дети);
* Места рождения, работы, домашние адреса близких родственников;
* Оклад и другие доходы;
* индивидуальный номер налогоплательщика;
* Номер пенсионного страхования;
* Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
* Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
* Информация о трудовой деятельности до приема на работу;
* Информация о знании иностранных языков;
* Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
* Данные о медицинской страховке;
* Данные об аттестации работников;
* Данные о повышении квалификации;
* Данные о наградах, медалях, поощрениях, почетных званиях;
* Информация о состоянии здоровья;
* Информация о негосударственном пенсионном обеспечении;
* Данные об имущественном и социальном положении;
* Сведения о доходах, имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера членов семьи;
* Сведения о социальных льготах и социальном статусе;
* Сведения о наличии (отсутствии) судимости;
* Номера расчетных счетов, банковских карт;
* Сведения о допуске к государственной тайне;
* Сведения о пребывание за границей.

Перечень персональных данных, обрабатываемых в администрации Малокамалинского сельсовета Рыбинского района в связи с оказанием муниципальных услуг и осуществлением муниципальных функций:

* Фамилия, Имя, Отчество;
* Дата рождения;
* Адрес регистрации (адрес проживания);
* Паспортные данные (серия, номер, кем и когда выдан);
* Семейное положение и состав семьи (муж/жена, дети);
* Оклад и другие доходы;
* номера контактных телефонов;
* адрес электронной почты;
* индивидуальный номер налогоплательщика;
* Номер пенсионного страхования;
* Имущественное положение;
* Социальное положение;
* Образование;
* Место работы;
* Причина и место смерти (серия, номер, кем выдано свидетельство о смерти, сведения об актовой записи).

Обезличенные и (или) общедоступные персональные данные:

-сведения о трудовой деятельности (общие данные о трудовой занятости на текущее время, общий и непрерывный стаж работы);

-сведения об образовании, квалификации, о наличии специальных знаний или специальной подготовки (дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками);

-сведения о повышении квалификации и переподготовке (дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения);

-сведения о заработной плате (в том числе данные по окладу, надбавкам, налогам);

— сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (военно-учетная специальность, воинское звание, данные о принятии/снятии с учета);

-сведения о семейном положении (состоянии в браке, наличие детей и их возраст);

— наличие (отсутствие) судимости.

Приложение № 6

к распоряжению

от 16.07.2025 № 48-о

**ПЕРЕЧЕНЬ**

должностей в администрации Малокамалинского сельсовета Рыбинского района , ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

 - глава сельсовета

- заместитель главы администрации

- специалист первой категории

Приложение № 7

к распоряжению

от 16.07.2025 № 48-о

**ПЕРЕЧЕНЬ**

должностей в администрации Малокамалинского сельсовета Рыбинского района, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

- глава муниципального образования;

- специалист первой категории;

- бухгалтер;

- работник ВУР.

Приложение № 8

к распоряжению

от 16.07.2025 № 48-о

**Форма обязательства**

о неразглашении информации, содержащей персональные данные

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество лица, допущенного к обработке персональных данных)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

исполняющий(ая) должностные обязанности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

предупрежден(а) о том, что на период исполнения должностных обязанностей мне будет предоставлен допуск к информации, содержащей персональные данные.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.
3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
5. В случае расторжения договора (контракта) и (или) прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что нарушение данного обязательства является основанием привлечения к дисциплинарной и(или) иной ответственности в соответствии с законодательством Российской Федерации.

Приложение 9

к распоряжению

от 16.07.2025 № 48-о

**ПОРЯДОК**

доступа муниципальных служащих и других работников администрации Малокамалинского сельсовета в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа муниципальных служащих и других работников администрации Малокамалинского сельсовета в помещения, в которых ведется обработка персональных данных (далее - Порядок), разработан в соответствии с Федеральным законом от 27.017.2006 № 152-ФЗ «О персональных данных», Приказом ФСБ России от 10.07.2014 г. № 378 «»Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 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» и другими нормативными правовыми актами.

2. Целью настоящего Порядка является исключение несанкционированного доступа к персональным данным субъектов персональных данных в администрации Малокамалинского сельсовета

3. Персональные данные относятся к конфиденциальной информации. Муниципальные служащие администрации Малокамалинского сельсовета получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные в информационной системе персональных данных и без использования средств автоматизации.

5. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

6. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только муниципальные служащие администрации Малокамалинского сельсовета, уполномоченные на обработку персональных данных.

Помещения оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня.

Хранение съемных машинных носителей персональных данных осуществлять в металлических шкафах, оборудованных внутренними замками с двумя дубликатами ключей и приспособленными для опечатывания замочных скважин.

7. Ответственными за организацию доступа в помещения, в которых ведется обработка персональных данных, является специалист 1 категории Малокамалинского сельсовета.

8. Нахождение лиц в помещениях администрации Малокамалинского сельсовета, не являющихся уполномоченными лицами на обработку персональных данных, возможно только при сопровождении уполномоченного специалиста администрации Малокамалинского сельсовета на время, ограниченное необходимостью решение вопросов, связанных с исполнением муниципальных функций и (или) осуществлением полномочий в рамках договоров, заключенных с администрацией Малокамалинского сельсовета.

9. Работники и должностные лица администрации Малокамалинского сельсовета, получившие доступ к персональным данным не должны покидать помещение, в котором ведется обработка персональных данных, оставляя в нем без присмотра посторонних лиц, включая работников, не уполномоченных на обработку персональных данных. После окончания рабочего дня дверь каждого помещения закрывается на ключ.

10. Внутренний контроль за соблюдением порядка доступа в помещения администрации Малокамалинского сельсовета, в которых ведется обработка персональных данных, проводится лицом, ответственным за организацию обработки персональных данных.

11. Перечень лиц, имеющих доступ в помещение, где ведется обработка персональных данных:

Прохорова Наталья Валерьевна, глава сельсовета - помещение № 1,2,3;

Перминова Елена Дмитриевна, специалист первой категории - помещение № 2;

Величко Чадура Кадыр-Ооловна, военно учетный работник - помещение № 3.

Приложение 10

к распоряжению

от 16.07.2025 № 48-о

**Типовая форма согласия на обработку персональных данных служащих, иных субъектов персональных данных**

Главе Малокамалинского сельсовета

Ф.И.О. руководителя

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

паспорт серии \_\_\_\_\_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_\_\_, выданный \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ « \_\_\_ » \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ года, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 21.03.2012 № 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» даю согласие администрации Малокамалинского сельсовета, расположенного по адресу: Красноярский край Рыбинский район с. Малая Камала ул. ул. Трактовая, 8 (далее – Оператор), на обработку в целях:

1) достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

2) осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

3) предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

4) исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

5) защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

6) осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

8) статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», при условии обязательного обезличивания персональных данных;

9) осуществления обработки персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

10) опубликования или обязательного раскрытия в соответствии с федеральным законом.

Мои персональные данные, в отношении которых дается данное согласие, включают:

1. Фамилия, имя, отчество (в том числе прежние с указанием даты, места и причины изменения).

2. Число, месяц, год и место рождения.

3. Фотография (3 x 4 см).

4. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство (в том числе прежнее с указанием даты, места и причины изменения), данные заграничного паспорта.

5. Домашний адрес (адрес регистрации, фактического проживания).

6. Номера телефонов (мобильного и домашнего) в случае их регистрации на субъекта персональных данных или по адресу его места жительства (по паспорту).

7. Сведения об образовании:

- время и названия оконченных учебных заведений, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому;

- послевузовское профессиональное образование: аспирантура, адъюнктура, докторантура (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);

- о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальности по окончании образовательного учреждения);

- знание иностранных языков и языков народов Российской Федерации (степень владения).

8. Сведения о выполняемой работе с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т.п.).

9. Сведения о воинской обязанности и воинское звание.

10. Сведения о допуске к государственной тайне с указанием периода работы, службы, учебы, оформления, его формы, номера и даты.

11. Сведения о пребывании за границей (когда, где, с какой целью).

12. Сведения о присвоенных классных чинах федеральной гражданской службы, дипломатических рангах, воинских или специальных званиях, классных чинах правоохранительной службы, классных чинах гражданской службы субъекта Российской Федерации, квалификационных разрядах государственной службы, квалификационных разрядах или классных чинах муниципальной службы (кем и когда присвоены).

13. Сведения о государственных наградах, иных наградах и знаках отличия.

14. Сведения о близких родственниках (отец, мать, братья, сестры и дети, муж (жена)), в том числе бывших, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство: фамилия, имя, отчество, сведения об изменении с указанием даты, места и причины изменения.

15. Сведения свидетельств о государственной регистрации актов гражданского состояния.

16. Номер страхового свидетельства обязательного пенсионного страхования.

17. ИНН.

18. Сведения страхового медицинского полиса обязательного медицинского страхования граждан.

19. Сведения о состоянии здоровья (форма N 001-ГС/У).

20. Справка о доходах, расходах, об имуществе и обязательствах имущественного характера муниципального служащего.

21. Сведения, указанные в оригиналах и копиях приказов по личному составу и материалам к ним.

22. Сведения экзаменационного, аттестационного листа муниципального служащего и отзывы об исполнении им должностных обязанностей за аттестационный период и уровне его знаний, навыков, умений (профессиональном уровне).

23. Сведения документов о начале служебной проверки, ее результатах, об отстранении муниципального служащего от замещаемой должности муниципальной службы.

24. Сведения трудового договора (контракта), а также дополнений и изменений, внесенных в трудовой договор (контракт).

25. Сведения о результатах проверки достоверности и полноты представленных муниципальным служащим сведений о доходах, расходах, об имуществе и обязательствах имущественного характера, а также сведений о соблюдении муниципальным служащим ограничений, установленных федеральными законами.

26. Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

27. Сведений о размещении информации в информационно-телекоммуникационной сети «Интернет».

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки:

- ввод, систематизация, хранение персональных данных (в электронном виде и на бумажном носителе);

- уточнение, обновление, изменение, модификация, обезличивание, блокирование, уничтожение персональных данных;

- использование персональных данных Оператором в связи со служебными отношениями;

- передача персональных данных работника третьим лицам в порядке, предусмотренном законодательством Российской Федерации.[[1]](#footnote-1)

С данными может производиться автоматизированная и неавтоматизированная обработка.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

В случае изменения моих персональных данных обязуюсь в пятнадцатидневный срок предоставить уточненные данные в наименование органа местного самоуправления.

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (дата) (подпись) (расшифровка)

**Типовая форма разъяснения юридических последствий отказа предоставить свои персональные данные**

Мне, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ разъяснены юридические  последствия   отказа   предоставить   свои   персональные   данные  наименование органа местного самоуправления.

В соответствии со статьями 16, 29 Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», статьями 57, 65 Трудового кодекса Российской Федерации субъект персональных данных, поступающих на работу или работающий в наименование органа местного самоуправления, обязан представить определенный перечень информации о себе.

Без предоставления субъектом персональных данных обязательных для заключения контракта (трудового договора) сведений, контракт (трудовой договор) не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской Федерации контракт (трудовой договор) прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности (продолжения работы).

 «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 дата подпись

Глава Малокамалинского сельсовета Н.В. Прохорова

Приложение 11

к распоряжению

от 16.07.2025 № 48-о

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБЪЕКТАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предмет Инструкции основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) Администрации Малокамалинского сельского поселения.

1.2. Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

# 2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

# ПОЛЬЗОВАТЕЛЬ ДОЛЖЕН:

2.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

- при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;

- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;

- оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

- не допускать "загрязнение" ПЭВМ посторонними программными средствами;

- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий,

- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;

- помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
* оценить необходимость дальнейшего использования файлов, зараженных вирусом;
* провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).
1. ЗАПРЕЩАЕМЫЕ ДЕЙСТВИЯ

ПОЛЬЗОВАТЕЛЬ НЕ ДОЛЖЕН:

3.1. Записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

- самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

- отключать (блокировать) средства защиты информации;

- производить какие-либо изменения в подключении и размещении технических средств;

- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

# ПРАВА ПОЛЬЗОВАТЕЛЯ ПЭВМ

# ПОЛЬЗОВАТЕЛЬ МОЖЕТ (ИМЕЕТ ПРАВО):

4.1. Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

4.2. Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

# 5. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ ПЭВМ

5.1. Пользователь несет ответственность за:

- надлежащее выполнение требований настоящей инструкции;

- соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

- сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;

- сохранность персональных данных.

Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

Приложение 12

к распоряжению

от 16.07.2025 № 48-о

**ПРАВИЛА**

рассмотрения запросов субъектов персональных данных

или их представителей в администрации Малокамалинского сельсовета Рыбинского района Красноярского края

1. Право субъектов персональных данных на получение сведений

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным *законодательством* Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с *законодательством* о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных *законодательством* Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Субъект персональных данных имеет право требовать от оператора уточнения его персональных данных, их блокирования или уничтожения, в случае если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

 2. Порядок предоставления оператором сведений по запросу субъекта персональных данных

1. При обращении либо при получении запроса субъекта персональных данных или его представителя сведения должны быть предоставлены в доступной форме. Запрос регистрируется в день поступления в установленном порядке.
2. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения, условное словесное обозначение и (или) иные сведения), либо сведения , иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.
3. Оператор при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных, обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными в течении 30 (тридцати) дней с даты получения запроса.

В случае отказа в предоставлении информации о наличии персональных данных оператор обязан дать в письменной форме мотивированный ответ с ссылкой на действующее законодательство, являющегося основанием для такого отказа. Отказ в предоставлении информации направляется в срок, не превышающий 30 (тридцати) дней со дня получения запроса субъекта персональных данных.

В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор в срок, не превышающий 7 (семь) рабочих дней, вносит в них необходимые изменения. О внесённых изменениях уведомляется субъект персональных данных или его представитель.

В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные в срок, не превышающий 7 (семь) рабочих дней. Об уничтоженных персональных данных уведомляется субъект персональных данных или его представитель.

При получении запроса из уполномоченного органа по защите прав субъектов персональных данных оператор обязан сообщить необходимую информацию в течении 30 (тридцати) дней с даты получения такого запроса.

 Возможность ознакомления с персональными данными предоставляется на безвозмездной основе лицом ответственным за обработку персональных данных.

Приложение № 13

к распоряжению

от 16.07.2025 № 48-о

**ИНСТРУКЦИЯ**

по организации антивирусной защиты в информационных системах персональных данных администрации Малокамалинского сельсовета Рыбинского района Красноярского края

1. Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты в информационных системах персональных данных (далее –ИСПДн) и устанавливает ответственность за их выполнение.

1. Основные определения

Вредоносное программное обеспечение (далее ПО) - специально разработанное программное обеспечение, программный модуль, блок, группа команд, имеющая способность к самораспространению, которая может попадать в общее и специальное программное обеспечение ИСПДн и приводить к:

- дезорганизации вычислительного процесса (нарушению или существенному замедлению обработки информации);

- модификации или уничтожению программ, или данных;

- приведению в негодность носителей информации и других технических средств;

- нарушению функционирования средств защиты информации.

1. Инструкция по применению средств антивирусной защиты

Защита ПО ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

* К использованию допускаются только лицензионные антивирусные средства, обладающие необходимой сертификацией в регулирующих органах РФ.
* Решение задач по установке и сопровождению средств антивирусной защиты возлагается на заместителя главы Малокамалинского сельсовета.
* Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
* Всё впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль.
* Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места.
* Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ИСПДн.
* Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов ИСПДн.
* Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.
* Контроль входящей информации необходимо проводить непосредственно после ее приема.
* Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
* Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
* При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции.
* При получении информации о возникновении вирусной эпидемии вне ИС должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.
* В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения вируса специалиста 1 категории Малокамалинского сельсовета;

- провести лечение зараженных файлов.

* По факту обнаружения зараженных вирусом файлов заместитель главы должен составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.
* Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.
* Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
* Ответственный за организацию обработки ПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.
* С данной инструкцией Пользователи должны быть ознакомлены под роспись в листе ознакомления с данной инструкцией.
* Проводить периодическое тестирование функций средств антивирусной защиты.
* Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

Приложение № 14

к распоряжению

от 16.07.2025 № 48-о

ПОРЯДОК

учета, хранения и уничтожения носителей персональных данных в администрации Малокамалинского сельсовета Рыбинского района

# 1.                  Термины и определения

В настоящем Порядке использованы следующие термины и определения:

**Информация**: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

**Конфиденциальная информация**: Информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.

**Конфиденциальность персональных данных:**Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

**Несанкционированный доступ (несанкционированные действия)**: Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

**Обработка персональных данных**: Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

**Персональные данные**: Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн) в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Пользователь персональных данных**: Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

**Процесс обработки персональных данных**: Процесс, в котором присутствует обработка персональных данных.

**Уничтожение персональных данных**: Действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

**Целостность информации**: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

# 2.        Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

|  |  |  |
| --- | --- | --- |
| № п/п | Сокращение | Описание |
| 1. | ИСПДн | Информационная система персональных данных |
| 2. | ОС | Операционная система |
| 3. | ПДн | Персональные данные |
| 4. | СВТ | Средство вычислительной техники |
| 5. | СЗПДн | Система защиты персональных данных |

# 3.      Область применения

Настоящий Порядок учета, хранения и уничтожения носителей ПДн (далее - Порядок) предназначен для определения единого порядка обращения с машинными (электронными) и бумажными носителями персональных данных в администрации Малокамалинского сельсовета Рыбинского района (далее ‑ Администрация).

# 4.      Общие положения

Настоящий Порядок устанавливает порядок учета, хранения, использования и уничтожения носителей ПДн в процессах обработки ПДн.

Настоящий Порядок разработан в соответствии с документом «Положение об обеспечении безопасности персональных данных в администрации муниципального образования Малокамалинского сельсовета Рыбинского района

# 5.    Порядок работы с бумажными носителями

## 5.1.     Порядок учета бумажных носителей, содержащих ПДн

Любой документ, содержащий ПДн, является конфиденциальным и подлежит обязательному учету. Учет документов, содержащих ПДн, осуществляется в соответствии с положениями настоящего Порядка.

Ответственность за организацию ведения учета документов возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

## 5.2.     Порядок хранения бумажных носителей, содержащих ПДн

С целью обеспечения физической сохранности документов, содержащих ПДн, предотвращения хищения документов, а также с целью недопущения разглашения содержащихся в них сведений документы должны храниться в местах, исключающих доступ к ним посторонних лиц.

Хранение открытых документов вместе с конфиденциальными документами разрешено только в случаях, когда они являются приложениями к конфиденциальным документам.

Рабочее место работника Администрация должно быть организовано таким образом, чтобы исключить возможность просмотра документов с ПДн лицами, которые не допущены к ПДн.

Во время работы на столе должны находиться только те документы, непосредственно с которыми ведется работа, все остальные должны быть убраны в места, предназначенные для хранения.

## 5.3.     Порядок уничтожения бумажных носителей, содержащих ПДн

Основанием для уничтожения документов, содержащих ПДн, является достижение целей обработки.

Локальные документы, содержащие ПДн, уничтожаются по мере необходимости.

Ответственность за своевременное уничтожение документов возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

Уничтожение документов производится с помощью специальных бумагорезательных технических средств (шредеров) или сжиганием.

* Уничтожение массивов документов

Массивы документов (архивы, библиотеки и т.п.) уничтожаются под контролем должностного лица ответственного за защиту ПДн.

Экспертиза документа проводится раз в год. Экспертиза охватывает все документы, содержащие ПДн, за соответствующий период времени.

Экспертиза проводится путем изучения содержания документов. Цель проведения экспертизы - определить возможность уничтожения документов либо дальнейшие сроки их хранения.

После проведения экспертизы составляется Акт о выделении дел
и документов, подлежащих уничтожению (Приложение А). В Акт включаются отобранные дела для уничтожения, отдельные документы из дел и документы выделенного хранения.

Уничтожение массивов документов производится с помощью бумагорезательных технических средств или сжиганием.

Если уничтожение массивов документов производит третья сторона,
с которой заключен соответствующий договор, то документы, выделенные для уничтожения, помещаются в короба, после чего короба запечатываются передаются третьей стороне.

После уничтожения массива документов должностными лицами ответственными за организацию работ по обработке ПД и за защиту ПДн, а также работниками производившими уничтожение документов подписывается Акт об уничтожении документов, содержащих ПДн (Приложение Б).

# 6.        Порядок работы с машинными носителями

Учету подлежат следующие типы машинных носителей ПДн:

* - отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD и прочее);
* - неотчуждаемые носители информации (жесткие магнитные диски).

## 6.1.     Порядок учета машинных носителей, содержащих ПДн

Все отчуждаемые машинные носители данных, используемые при работе со средствами вычислительной техники (далее ‑ СВТ) для обработки и хранения ПДн, обязательно регистрируются и учитываются в **Журнале учета выдачи машинных носителей ПДн (Приложение В)**.

Неотчуждаемые носители информации подлежат учету в составе системных блоков СВТ, которые в свою очередь учитываются в Техническом паспорте ИСПДн.

Ответственность за ведение Журнала учеты выдачи машинных носителей ПДн и контроль учета носителей ПДн возлагается на системного администратора Администрации.

Каждому машинному носителю, содержащему ПДн, присваивается учетный номер согласно Журналу.

В качестве учетного номера допускается использование серийного (заводского) номера носителя. В случае отсутствия серийного номера, учетный номер наносится на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

## 6.2.     Порядок использования машинных носителей ПДн

Машинные носители ПДн выдаются пользователям или другим лицам, участвующим в обработке ПДн, для работы под подпись в Журнале. По завершении работы машинные носители ПДн сдаются обратно.

В случае повреждения машинных носителей ПДн, работник, за которым закреплен носитель, сообщает о случившемся должностному лицу ответственному за защиту ПДн.

Передача носителя, содержащего ПДн, третьим сторонам производится в соответствии с требованиями договора между Администрация и третьим лицом.

Машинные носители ПДн пересылаются в том же порядке, что и документы.

При фиксации ПДн на машинных носителях не допускается фиксация на одном машинном носителе ПДн, цели обработки которых заведомо не совместимы.

Вынос машинных носителей, содержащих ПДн, за пределы контролируемой зоны Администрация запрещается без соответствующего разрешения должностного лица ответственного за защиту ПДн.

## 6.3.     Порядок хранения машинных носителей ПДн

Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, нарушения целостности или уничтожения содержащейся на них информации.

Отчуждаемые съемные носители после окончания работы с ними должны убираться в сейфы или металлические шкафы, запираемые на ключ.

Не допускается оставлять без присмотра на рабочем столе или в СВТ машинные носители, содержащие ПДн.

Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа к записанным на них ПДн несет работник, за которым закреплен носитель.

## 6.4.        Порядок уничтожения машинных носителей ПДн

Основанием для уничтожения машинных носителей ПДн, является повреждение машинного носителя, исключающее его дальнейшее использование, или потеря практической ценности носителя. Решение об уничтожении машинного носителя принимает должностное лицо ответственное за защиту ПДн.

Списанные машинные носители, подлежащие уничтожению, хранятся в сейфе должностного лица ответственного за защиту ПДн. Уничтожение таких носителей производится раз в год.

Уничтожение носителей производится путем их физического разрушения с предварительным затиранием (форматированием, уничтожением) содержащихся на них ПДн, если это позволяют физические принципы работы носителя.

Уничтожение машинных носителей производится Комиссией в составе не менее 3 человек. В состав Комиссии должно обязательно входить должностное лицо ответственное за защиту ПДн. После уничтожения всех машинных носителей составляется **Акт об уничтожении персональных данных (Приложение Г)**.

При уничтожении, машинные носители снимаются с учета. Отметка об уничтожении носителей проставляется в Журнале.

## 6.5.     Порядок уничтожения (стирания) ПДн с машинного носителя

Основанием для уничтожения (стирания) записей или части записей с электронного носителя являются следующие случаи:

* - возврат носителя сотрудником;
* - передача носителя в ремонт;
* - списание носителя.

Хранящаяся на электронных носителях и потерявшая актуальность информация, содержащая ПДн, своевременно стирается (уничтожается). Работник, совместно с системным администратором Администрации, принимает окончательное решение о необходимости уничтожения (стирания) с него записей.

Работник осуществляет уничтожение информации с носителя самостоятельно, с использованием встроенных средств ОС.

При невозможности самостоятельного уничтожения информации с носителя, работник передает электронный носитель должностному лицу ответственному за защиту ПДн. Совместно с носителем передается служебная записка, в которой указывается причины передачи (возврата) и основание для уничтожения содержащейся на нем информации.

Должностное лицо ответственное за защиту ПДн, ответственное за уничтожение (стирание) информации с электронных носителей, при получении носителя должно обеспечить уничтожение (стирание) информации с носителя, способом, исключающим ее дальнейшее восстановление и подготовить **Акт об уничтожении персональных данных (Приложение Г)**.

В Акт заносится дата, учетный номер носителя и способ уничтожения (стирания) информации, а также используемые для этого программные средства.

Носители, пригодные к повторной эксплуатации, после уничтожения записанной на них информации могут быть использованы для повторной записи информации.

# 7.        Пересмотр и внесение изменений

Пересмотр положений настоящего документа проводится в следующих случаях:

* - при появлении новых требований к обработке и обеспечению безопасности ПДн со стороны законодательства РФ и контролирующих органов исполнительной власти Российской Федерации;
* - по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;
* - по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;
* - не реже одного раза в год.

Ответственным за пересмотр настоящего Порядка и составление рекомендаций по изменению является должностное лицо ответственное за защиту ПДн.

Внесение изменений производится на основании соответствующего распоряжения администрации муниципального образования Малокамалинского сельсовета Рыбинского района

**\_\_\_\_\_\_\_\_\_\_\_\_**

# Приложение А

**А К Т № \_\_\_\_\_\_**

**о выделении дел и документов, подлежащих уничтожению**

от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

Комиссия в составе:

<Фамилия И.О. – должность;>

<Фамилия И.О. – должность.>

<Фамилия И.О. – должность.>

составила настоящий акт о том, что на основании проведенной экспертизы, отобрала к уничтожению, следующие документы и дела, утратившие практическую ценность:

|  |  |  |
| --- | --- | --- |
| № п\п | Заголовок документа\дела | Основание для уничтожения |
|   |   |   |
|   |   |   |
|   |   |   |

|  |  |  |
| --- | --- | --- |
|   |   |   |
| Члены комиссии: |   |   |
|   | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|   |   |   |
|   | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|   |   |   |
|   | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

#

# Приложение Б

**А К Т № \_\_\_\_\_\_**

**уничтожения бумажных носителей, содержащих**

**персональные данные**

от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

Комиссия в составе:

<Фамилия И.О. – должность;>

<Фамилия И.О. – должность.>

<Фамилия И.О. – должность.>

составила настоящий акт о том, что произведено плановое уничтожение бумажных носителей, содержащих персональные данные, с истекшим сроком использования и/или утративших практическое значение.

* «тип носителя, учётный номер носителя»
* «тип носителя, учётный номер носителя»
* …

Бумажные носители уничтожены путём сжигания/шредирования/химической обработки и т.п. (нужное отметить).

|  |  |  |
| --- | --- | --- |
|    |   |   |
| Члены комиссии |   |   |
|   | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|   |   |   |
|   | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|   |   |   |
|   | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

#

# Приложение В

**Журнал учета носителей информации, содержащих персональные данные**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Учетный № носителя | Дата | Тип носителя | Содержимое носителя | Ф.И.О.отв. лица | Подпись отв. лица | Отметка о возврате (с указанием причины) | Ф.И.О. отв. лица | Подпись отв. лица | Дата уничтожения носителя | Ф.И.О. отв. за уничтожение |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |

#

# Приложение Г

|  |
| --- |
|  УТВЕРЖДАЮ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Глава муниципального образования\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись)«\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г. |

#

# Акт об уничтожении персональных данных

Комиссия в составе:

Председатель – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п/п | Дата | Тип носителя | Регистрационный номерносителя ПДн | Примечание |
|   |   |   |   |   |
|   |   |   |   |   |

Всего съемных носителей \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_/

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_/

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_/

 Приложение № 15

к распоряжению

от 16.07.2025 № 48-о

ПОРЯДОК

реагирования на инциденты информационной безопасности в администрации Малокамалинского сельсовета Рыбинского района

# 1.        Термины и определения

В настоящем Порядке использованы следующие термины и определения:

**Безопасность персональных данных**: Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Блокирование персональных данных**: Временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

**Вредоносное программное обеспечение**: Программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Доступ к информации**: Возможность получения информации и ее использования.

**Защита информации**: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

**Идентификация**: Присвоение субъектам и объектам доступа идентификатора
и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информационная система персональных данных:**Информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таковых средств**.**

**Информация**: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**.**

**Использование персональных данных**: Действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом, затрагивающих права и свободы субъекта ПДн или других лиц**.**

**Конфиденциальность персональных данных:**Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

**Несанкционированный доступ (несанкционированные действия)**: Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

**Обработка персональных данных**: Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

**Персональные данные**: Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн) в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Пользователь персональных данных**: Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

**Процесс обработки персональных данных**: Процесс, в котором присутствует обработка персональных данных.

**Средство защиты информации**: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**Уничтожение персональных данных**: Действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

**Целостность информации**: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

**Доступность информации**- Свойство информационной безопасности, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

# 2.        Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

|  |  |  |
| --- | --- | --- |
| № п/п | Сокращение | Описание |
| 1. | ИБ | Информационная безопасность |
| 2. | ИСПДн | Информационная система ПДн |
| 3. | НСД | Несанкционированный доступ |
| 4. | ПДн | Персональные данные |

# 3.        Область применения

Настоящий Порядок реагирования на инциденты информационной безопасности (далее - Порядок) предназначен для определения единого порядка реагирования на возникшие инциденты информационной безопасности, проведения служебных расследований, а также проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в администрации Малокамалинского сельсовета Рыбинского района (далее по тексту - администрация).

Требования настоящего Порядка распространяются на должностных лиц администрации, отвечающие за обеспечение безопасности ПДн.

# 4.    Общие положения

Настоящий Порядок разработан в соответствии с Политикой администрации Малокамалинского сельсовета Рыбинского района в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

В соответствии с настоящим Порядком к инцидентам ИБ в администрации относятся:

* - нарушение конфиденциальности, целостности или доступности ПДн;

- отказ оборудования, сервисов, средств обработки и (или), входящих в состав ИСПДн;

* - несоблюдение требований внутренних организационно-распорядительных документов и действующих нормативных документов РФ в области обработки и защиты ПДн (нарушение правил обработки ПДн);
* - заражение программных компонентов ИСПДн вредоносным программным обеспечением.

К инцидентам ИБ в ИСПДн также относятся попытки и факты получения НСД к ИСПДн:

* - сеансы работы в ИСПДн незарегистрированных пользователей;

- сеансы работы Пользователей ИСПДн, срок действия полномочий, которых истек, либо в состав полномочий, которых не входят выявленные действия с ПДн;

- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой выгоды, методом подбора пароля или иными методами (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

- совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);

- несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки, или защиты, входящих в состав ИСПДн.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для возникновения описанных выше инцидентов.

# 5.        Оповещение об инциденте информационной безопасности

В случае выявления инцидента ИБ устанавливается следующая последовательность действий сотрудников администрации:

* прекратить работу с ресурсом, в котором выявлен инцидент ИБ;
* оповестить своего непосредственного руководителя о факте выявления инцидента ИБ;
* руководитель должен оповестить должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн;
* после извещения указанных должностных лиц по их требованию предоставить всю необходимую информацию.

Должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его возникновению, и составляет краткую справку, в которой описывается произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ. Справка направляется главе администрации для принятия решения о проведении расследования инцидента ИБ.

Порядок проведения расследования инцидента ИБ описан в разделе 7 настоящего документа.

Мероприятия по устранению причин и недопущению повторного возникновения инцидента ИБ описаны в разделе 8 настоящего документа.

1. Мероприятия при возникновении инцидента информационной безопасности, ставшего причиной возникновения негативных последствий для субъекта ПДн

В случае если инцидент ИБ может стать (или уже стал) причиной возникновения негативных последствий для субъектов ПДн, необходимо немедленно блокировать ПДн этих субъектов до устранения причин, повлекших за собой возникновение инцидента ИБ. Решение о блокировании ПДн принимает должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн.

ПДн остаются заблокированными до устранения причин, повлекших за собой возникновение инцидента ИБ.

# 7.        Проведение расследования инцидента информационной безопасности

Внутреннее расследование и составление заключений должно в обязательном порядке проводиться в случае выявления:

- нарушения конфиденциальности, целостности или доступности ПДн;

- халатности и несоблюдения требований по обеспечению безопасности ПДн;

- несоблюдения условий хранения носителей ПДн;

- использования СЗИ, которые могут привести к нарушению заданных характеристик безопасности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

Задачами внутреннего расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

- установление лиц, непосредственно виновных в данном нарушении;

- выявление причин и условий, способствовавших нарушению.

Проведение внутреннего расследования проводится по распоряжению главы муниципального образования. С целью проведения расследования в обязательном порядке формируется Комиссия, в состав которой входят должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн, юрист и иные должностные лица администрации, участие которых может потребоваться.

Комиссия должна приступить к работе по расследованию не позднее следующего рабочего дня после даты выявления инцидента ИБ.

Общая продолжительность внутреннего расследования не должна превышать одного месяца.

В рамках проведения расследования инцидента ИБ Комиссия уполномочена:

- проводить опрос сотрудников администрации, по вине которых предположительно произошел инцидент ИБ, а также должностных лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;

- проводить осмотр объектов и предметов, которые могут иметь отношение к инциденту ИБ;

По решению главы администрации на Комиссию могут быть возложены дополнительные обязанности и права.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с распоряжением о проведении расследования.

Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (акты, протоколы, справки и т.п.).

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии в виде протокола.

В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения главой администрации.

Для оперативного проведения внутреннего расследования должностное лицо ответственного за защиту ПДн составляет План проведения расследования.

Одновременно с проведением внутреннего расследования, глава администрации может поручить Комиссии определить ущерб для администрации и (или) для субъекта ПДн от произошедшего инцидента ИБ. В отдельных случаях такая оценка может быть осуществлена с привлечением специализированной организации.

По окончании внутреннего расследования Комиссия представляет главе администрации отчет по результатам расследования, в котором излагаются:

* - основания и время проведения расследования;
* - проделанная работа (кратко);
* - время, место и обстоятельства факта нарушения;
* - причины и условия совершения нарушения;
* - виновные лица и степень их вины;
* - наличие умысла в действиях виновных лиц;
* - предложения по возмещению ущерба;
	+ - предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
* - рекомендации по исключению подобных нарушений;
	+ - другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т. д.).

К отчету прилагаются:

* - письменные объяснения лиц, которых опрашивали члены Комиссии;

- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т. д.;

- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба.

Отчет должен быть подписан всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Отчет подлежит утверждению главой администрации.

Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право ознакомления с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с отчетом по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

При наличии в действиях работника признаков административного правонарушения или уголовного преступления глава администрации обязан обратиться в правоохранительные органы для привлечения виновного к ответственности, в соответствии с положениями нормативных документов РФ.

В соответствии с Трудовым кодексом РФ, возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нанесение ущерба.

Первый экземпляр отчета с резолюцией главы администрации, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дела о внутренних расследованиях хранятся у главы администрации.

# 8.        Превентивные меры по недопущению повторного возникновения инцидентов информационной безопасности

Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение, в зависимости от произошедшего инцидента ИБ, включают в себя:

* - мониторинг событий в информационной системе ПДн;
* - своевременное удаление неиспользуемых учетных записей;

- контроль и мониторинг действий пользователей в информационной системе ПДн;

- проведение обучения (повторного обучения) пользователей правилам обработки и обеспечения безопасности ПДн;

- ознакомление пользователей с мерами ответственности, установленными нормативными документами РФ, за нарушение норм и правил обработки ПДн, а также за разглашение полученных данных.

# 9.        Пересмотр и внесение изменений

Настоящий Порядок должен пересматриваться в случаях:

- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;

- по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;

- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;

Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн в администрации.

Внесение изменений производится на основании соответствующего распоряжения администрации.

Приложение 16

к распоряжению

от 16.07.2025 № 48-о

|  |  |  |
| --- | --- | --- |
|  |  | **УТВЕРЖДАЮ** |
|  |  | Глава Малокамалинского сельсовета |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Н.В. Прохорова |
|  |  | «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |

# ЖУРНАЛ

**ОЗНАКОМЛЕНИЯ РАБОТНИКОВ**

**С ЛОКАЛЬНЫМИ НОРМАТИВНЫМИ АКТАМИ**

**В ОБЛАСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Начат «      » 20          г.

Окончен «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Фамилия, имя, отчество работника | Должность работника | Отметка об ознакомлении |
| Подпись работника | Дата ознакомления |
| 1. **Правила** осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
2. Правила работы с обезличенными персональными данными в администрации Малокамалинского сельсовета Рыбинского района Красноярского края
3. Перечень лиц, допущенных к обработке персональных данных в информационной системе персональных данных администрации Малокамалинского сельсовета
4. **Перечень** персональных данных, обрабатываемых в администрации Малокамалинского сельсовета Рыбинского района в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций
5. **Перечень** должностей в администрации Малокамалинского сельсовета Рыбинского района , ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных
6. П**еречень** должностей в администрации Малокамалинского сельсовета Рыбинского района, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным
7. Порядок доступа муниципальных служащих и других работников администрации Малокамалинского сельсовета в помещения, в которых ведется обработка персональных данных
8. Типовую форму согласия на обработку персональных данных служащих, иных субъектов персональных данных, а также типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в администрацию Малокамалинского сельсовета
9. Инструкцию пользователя при обработке персональных данных на объектах вычислительной техники
10. **Правила** рассмотрения запросов субъектов персональных данных или их представителей в администрации Малокамалинского сельсовета Рыбинского района
11. Инструкциюпо организации антивирусной защиты в информационных системах персональных данных администрации Малокамалинского сельсовета Рыбинского района
12. Порядок учета, хранения и уничтожения носителей персональных данных в администрации Малокамалинского сельсовета Рыбинского района
13. Порядок реагирования на инциденты информационной безопасности в администрации Малокамалинского сельсовета Рыбинского района
 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. [↑](#footnote-ref-1)