

РОССИЙСКАЯ ФЕДЕРАЦИЯ  
КОСТРОМСКАЯ ОБЛАСТЬ



АДМИНИСТРАЦИЯ МАКАРЬЕВСКОГО  
МУНИЦИПАЛЬНОГО ОКРУГА

РАСПОРЯЖЕНИЕ

От 21.02.2025

№ 88-РА

Об обеспечении безопасности информации при обработке персональных данных в администрации Макарьевского муниципального округа Костромской области

В целях исполнения требований Федерального закона от 27 июля 2006 года № 252-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 21 марта 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативно правовыми актами, операторами, являющимися государственными или муниципальными органами», в соответствии с Законом Костромской области от 21.05.2024 № 478-7-ЗКО «О преобразовании муниципальных образований, входящих в состав Макарьевского муниципального района Костромской области, и внесении изменений в отдельные законодательные акты Костромской области»:

1. Утвердить:

1.1. список ответственных лиц за сбор, обработку и хранение материалов персональных данных работников администрации Макарьевского муниципального округа Костромской области (Приложение № 1).

1.2. список ответственных лиц за сбор, обработку и хранение персональных данных контрагентов администрации Макарьевского муниципального округа (Приложение № 2).

1.3. места хранения материальных носителей персональных данных (Приложение № 3)

1.4. положение по обработке и защите персональных данных работников в администрации Макарьевского муниципального округа Костромской области (Приложение № 4).

1.5. перечень персональных данных, обрабатываемых в администрации Макарьевского муниципального округа Костромской области (Приложение № 5).

1.6. инструкцию пользователя информационной системой персональных данных в администрации Макарьевского муниципального округа Костромской области (Приложение № 6).

1.7. типовую форму согласия на обработку персональных данных работниками администрации Макарьевского муниципального округа Костромской области (Приложение № 7).

1.8. форму дополнительного соглашения к служебному контракту (обязательство муниципального служащего администрации Макарьевского муниципального округа Костромской области, непосредственно осуществляющего обработку персональных данных) (Приложение № 8).

1.9. перечень информационных систем персональных данных, обрабатываемых в администрации Макарьевского муниципального округа (Приложение № 9).

1.10. перечень должностей администрации Макарьевского муниципального округа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (Приложение № 10).

2. Признать утратившими силу распоряжения администрации Макарьевского муниципального района:

- от 20.04.2012 № 173-Р «Об обеспечении безопасности информации при обработке персональных данных в администрации Макарьевского муниципального района Костромской области»;

от 04.07.2012 № 279-РА «О внесении изменений в распоряжение администрации Макарьевского муниципального района от 20.04.2012 № 173-Р»;

- от 03.08.2015 № 220-Р «О внесении изменений в распоряжение администрации Макарьевского муниципального района от 20.04.2012 № 173-Р»;

- от 31.12.2019 № 576-РА «О внесении изменений в распоряжение администрации Макарьевского муниципального района от 20.04.2012 № 173-Р «Об обеспечении безопасности информации при обработке персональных данных в администрации Макарьевского муниципального района Костромской области»;

- от 30.12.2020 № 520-РА «О внесении изменений в распоряжение администрации Макарьевского муниципального района от 20.04.2012 № 173-Р «Об обеспечении безопасности информации при обработке персональных данных в администрации Макарьевского муниципального района Костромской области».

3. Контроль исполнения настоящего распоряжения оставляю за собой.

4. Настоящее распоряжение вступает в силу со дня подписания.

Глава Макарьевского муниципального округа  
Костромской области

А.Н. Казвиров

Список ответственных лиц за сбор, обработку и хранение материалов  
персональных данных работников администрации  
Макарьевского муниципального округа Костромской области

1. Суркова Светлана Сергеевна – управляющий делами администрации Макарьевского муниципального округа, в части обработки личных дел работников администрации Макарьевского муниципального округа в соответствии с Трудовым кодексом РФ, Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации»;

2. Нефёдова Татьяна Александровна - главный бухгалтер отдела бухгалтерского учета и отчетности, в части обработки карточек-справок по форме 0504417, форм отчетности в пенсионный фонд, фонд социального страхования, налоговую инспекцию в соответствии с Налоговым кодексом Российской Федерации, Бюджетным кодексом Российской Федерации, Постановлением Правления ПФР от 01.12.2010 № 157Н, Приказом Минфина от 29.12.2007 № 163н, Приказом ФНС от 09.11.2006 № САЭ-3-10/777;

3. Мухина Лилия Николаевна – главный специалист отдела по мобилизационной работе, ГО и ЧС, в части обработки персональных данных работников администрации Макарьевского муниципального округа в соответствии с Федеральным законом от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе».

Список ответственных лиц за сбор, обработку и хранение персональных данных контрагентов администрации Макарьевского муниципального округа

1. Нефёдова Татьяна Александровна - главный бухгалтер отдела бухгалтерского учета и отчетности в части обработки карточек-справок по форме 0504417, форм отчетности в пенсионный фонд, фонд социального страхования, налоговую инспекцию в соответствии с налоговым кодексом РФ, Бюджетным кодексом РФ, Постановлением Правления ПФР от 01.12.2010 № 157Н, Приказом Минфина от 29.12.2007 № 163н, Приказом ФНС от 09.11.2006 № САЭ-3-10/777.

2. Швакова Светлана Павловна – секретарь руководителя управления по обращениям граждан, информатизации и связи администрации Макарьевского муниципального округа, в части обработки карточек, поступивших в администрацию Макарьевского муниципального округа обращений граждан, в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

3. Братанова Екатерина Андреевна - секретарь административной комиссии, в части обработки материалов административной комиссии, в соответствии с законом Костромской области от 21.07.2008 № 352-4-ЗКО «Кодекс Костромской области об административных правонарушениях»;

4. Уткина Елена Валентиновна - ответственный секретарь комиссии по делам несовершеннолетних и защите их прав, в части обработки материалов комиссии по делам несовершеннолетних и защите их прав, в соответствии с Федеральным законом от 19.05.1995 № 82-ФЗ «Об общественных объединениях».

5. Бурлак Юлия Борисовна - главный специалист отдела инфраструктуры и ЖКХ администрации Макарьевского муниципального округа, в части обработки персональных данных граждан, признанных в установленном действующим законодательстве порядке нуждающимися в жилых помещениях, предоставляемых по договорам социального найма, в соответствии с Жилищным кодексом Российской Федерации.

Места хранения  
материальных носителей персональных данных

1. Металлический шкаф № 3 каб. № 201 (г. Макарьев, пл. Революции, д. 8), для хранения личных дел работников администрации Макарьевского муниципального округа;

2. Металлический шкаф № 1 каб. № 205 (г. Макарьев, пл. Революции, д. 8), для хранения карточек-справок по форме 0504417, форм отчетности в пенсионный фонд, фонд социального страхования, налоговую инспекцию;

3. Сейф № 1 каб. № 204 приемная (г. Макарьев, пл. Революции, д. 8), для хранения карточек, поступивших в администрацию Макарьевского муниципального округа обращений граждан;

4. Металлический шкаф № 3 и сейф № 2 каб. № 107 (г. Макарьев, пл. Революции, д. 8);

5. Металлический шкаф № 1 каб. № 201 (г. Макарьев, пл. Революции, д. 8), для хранения персональных данных и материалов административной комиссии Макарьевского муниципального округа;

6. Сейф № 1 каб. № 115 (г. Макарьев, пл. Революции, д. 8), для хранения персональных данных и материалов комиссии по делам несовершеннолетних и защите их прав.

## ПОЛОЖЕНИЕ

об обработке и защите персональных данных работников администрации  
Макарьевского муниципального округа Костромской области

### 1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона » от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие распоряжением администрации Макарьевского муниципального округа и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

### 2. Понятие и состав персональных данных

2.1. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:

- фамилия, имя, отчество;
- дата рождения;
- гражданство;
- сведения об образовании, о дополнительном профессиональном образовании, присвоении ученой степени, ученого звания;
- идентификационный номер налогоплательщика (ИНН);
- номер страхового свидетельства государственного пенсионного страхования;
- номер паспорта или заменяющего его документа, дата выдачи;
- домашний адрес регистрации;
- сведения о трудовой деятельности;
- сведения об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению;
- сведения о доходах и имуществе, принадлежащих муниципальным служащим администрации Макарьевского муниципального округа;

- сведения о доходах и имуществе, принадлежащих супругу (супруге) и несовершеннолетним детям на праве собственности, муниципальных служащих и администрации Макарьевского муниципального округа.

2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

### 3. Обработка персональных данных

3.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

3.2.4. Персональные данные следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

3.2.6. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

- Управляющий делами администрации Макарьевского муниципального округа;
- Начальник управления по обращениям граждан, информатизации и связи администрации Макарьевского муниципального округа;
- Отдела бухгалтерского учета и отчетности администрации Макарьевского муниципального округа;
- Отдела по мобилизационной работе, ГО и ЧС.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.5. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным распоряжением по администрации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.5.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.5.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы администрации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.9. При принятии решений, затрагивающих интересы работника,

работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

#### 4. Доступ к персональным данным

##### 4.1. Внутренний доступ (доступ внутри организации).

##### 4.1.1. Право доступа к персональным данным сотрудника имеют:

- глава Макарьевского муниципального округа;
- заместители главы администрации Макарьевского муниципального округа;
- управляющий делами администрации Макарьевского муниципального округа;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- сам работник, носитель данных.
- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется распоряжением главы Макарьевского муниципального округа.

##### 4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального Фонда России.

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

##### 4.2.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

#### 5. Защита персональных данных

5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное

проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности администрации.

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.5. «Внутренняя защита».

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами администрации.

5.5.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками администрации по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только главе Макарьевского муниципального округа, заместителям главы администрации Макарьевского муниципального округа, управляющему делами администрации Макарьевского муниципального округа; и в исключительных случаях, по письменному разрешению Главы Макарьевского муниципального округа, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть

защищены паролем, который сообщается управляющему делами администрации Макарьевского муниципального округа и начальнику управления по обращениям граждан, информатизации и связи администрации Макарьевского муниципального округа.

#### 5.6. «Внешняя защита».

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности администрации, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут выработать совместные меры защиты персональных данных работников.

## 6. Права и обязанности работника

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2. Работники и их представители должны быть ознакомлены под расписку с документами администрации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

6.4. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных,

документированных персональных данных, состав которых установлен Трудовым кодексом РФ.

- своевременно сообщать работодателю об изменении своих персональных данных.

6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

## 7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник администрации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной

жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

**ПЕРЕЧЕНЬ**  
персональных данных, обрабатываемых в администрации  
Макарьевского муниципального округа Костромской области

№ п/п	Наименование (вид) ПДн	Содержание персональных данных (ПД)	Категория ПДн	Источник получения	Основание для обработки ПДн	Технологический процесс, использующий вид ПДн	Срок хранения, условия прекращения обработки	Общедоступность
1	<b>Персональные данные работников</b>							
1.1	Первичные учетные данные работников	ФИО работника	4 категория	- Субъект ПДн - Паспорт - Страховое свидетельство - ИНН - Диплом об образовании - Заявление о приеме на работу - Трудовая книжка	Трудовое законодательство РФ, согласие субъекта ПДн	Прием сотрудника на работу Увольнение работника Начисление работнику зарплаты Начисление работнику премии	На период работы, 75 лет после увольнения	Общедоступные
1.2	Сведения о занимаемой должности	- наименование структурного подразделения - наименование занимаемой должности	4 категория	- Субъект ПДн - Трудовой договор - трудовая книжка	Трудовое законодательство РФ, согласие субъекта ПДн	Прием сотрудника на работу Увольнение работника Начисление работнику зарплаты Начисление работнику премии	На период работы, 75 лет после увольнения	Общедоступные
1.3	Финансовое состояние работника	Сведения о текущем должностном окладе	3 категория	- Субъект ПДн - Трудовой договор - приказ о премиях	Трудовое законодательство РФ, согласие субъекта ПДн	Прием сотрудника на работу Увольнение работника Начисление работнику зарплаты	На период работы, 75 лет после увольнения	Не общедоступные
1.4	Сведения о реквизитах работника	- дата рождения - адрес прописки - ИНН - данные паспорта - номер страхового свидетельства	3 категория	- Субъект ПДн, - трудовой договор, - трудовая книжка, - паспорт, - страховое свидетельство	Трудовое законодательство РФ, согласие субъекта ПДн	Прием сотрудника на работу Увольнение работника Начисление работнику зарплаты	На период работы, 75 лет после увольнения	Не общедоступные

1.5	Дополнительные сведения о работнике	- данные об образовании - данные о детях - данные о семейном положении	3 категория	- Субъект ПДн, - дипломы, - паспорт	Трудовое законодательство РФ, согласие субъекта ПДн	Прием сотрудника на работу Увольнение работника Начисление работнику заработной платы Начисление работнику премии	На период работы, 75 лет после увольнения	Не общедоступные
2	<b>Персональные данные контрагентов</b>							
2.1	Первичные учетные данные представителей контрагентов	ФИО контрагента	3 категория	Субъект ПДн, паспорт	- Согласие субъекта ПДн	Регистрация в базе ЕСЭД Изменение данных о клиенте Выдача справки клиенту	5 лет	Не общедоступные
2.2	Сведения о реквизитах контрагента	- адрес прописки - данные паспорта - номер телефона	2 категория	Субъект ПДн, паспорт	- Согласие субъекта ПДн	Регистрация в базе ЕСЭД Изменение данных о клиенте Выдача справки клиенту	5 лет	Не общедоступные

**ИНСТРУКЦИЯ**  
пользователя информационной системы персональных данных в администрации  
Макарьевского муниципального округа Костромской области

1. Общие положения

Настоящая Инструкция разработана для обеспечения защиты персональных данных в администрации Макарьевского муниципального округа Костромской области.

Персональные данные (ПДн) относятся к категории информации ограниченного распространения.

Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств, с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с персональными данными строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;
- принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. Обязанности работников, имеющих доступ к ПДн.

Работники, получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных данных немедленно информировать руководителя структурного подразделения, специалиста по защите информации.

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности администрации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности администрации Макарьевского муниципального округа, полученные в течение срока работы.

Работники при работе с персональными данными обязаны:

- 1) Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
  - 2) Выполнять требования администратора безопасности, касающиеся защиты информации;
  - 3) Знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;
  - 4) Хранить в тайне свой аудентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;
  - 5) Использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и т.д.);
  - 6) Контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности, ответственному за антивирусную защиту автоматизированной системы;
  - 7) Немедленно ставить в известность руководителя подразделения:
    - в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;
    - нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИСПДн;
    - несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн.
  - 8) В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.
  - 9) Ставить в известность администратора безопасности структурного подразделения при:
    - необходимости обновления антивирусных баз;
    - обновлении программного обеспечения;
    - проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;
    - необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;
    - резервном копировании информации;
    - и т.д.
- Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.
- Вынос ПЭВМ, на которой проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с руководителем подразделения запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.
- ПЭВМ, используемые для работы с персональными данными, должны быть

размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения ограниченного распространения;
- использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;
- накапливать ненужные для работы персональные данные;
- передавать или принимать без расписки документы ограниченного распространения;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера.
- использовать компоненты программного и аппаратного обеспечения ИСПДн подразделения в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить персональные данные на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения, ответственного за техническое и (или) программное обеспечение, администратора безопасности.

### 3. Ответственность

Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

## ЗАЯВЛЕНИЕ

Я, \_\_\_\_\_  
(фамилия, имя, отчество)

\_\_\_\_\_

(адрес прописки, регистрации)

\_\_\_\_\_

(вид документа, удостоверяющий личность)

с целью заключения служебного контракта и получения справок  
(указать цели обработки персональных данных)

Даю согласие на обработку своих персональных данных:

\_\_\_\_\_

(указать перечень персональных данных, на обработку которых дается согласие субъекта персональных данных)

*фамилия, имя, отчество, дата рождения, гражданство, сведения об образовании, о дополнительном профессиональном образовании, о присвоении ученой степени, ученого звания, идентификационный номер (ИНН), номер страхового свидетельства государственного пенсионного страхования, номер паспорта или заменяющего его документа, дата выдачи, домашний адрес регистрации, сведения о трудовой деятельности, сведения об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению, сведения из органов государственной налоговой службы о доходах и имуществе, принадлежащем гражданину на праве собственности, сведения о доходах супруга (супруги) и несовершеннолетних детей*

в документарной и электронной форме, с возможностью осуществления сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения персональных данных, автоматизированным и неавтоматизированным способом.

Настоящее согласие действительно на период действия контракта.

Настоящее согласие может быть отозвано мной в письменной форме. В случае отзыва настоящего согласия до окончания срока его действия, я предупрежден о возможных последствиях прекращения обработки своих персональных данных.

Дата \_\_\_\_\_

Подпись \_\_\_\_\_

**ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ**  
к служебному контракту № \_\_\_\_\_ от \_\_\_\_\_  
(обязательство служащего администрации Макарьевского муниципального округа,  
непосредственно осуществляющего обработку персональных данных)

г. Макарьев

Администрация Макарьевского муниципального округа в лице \_\_\_\_\_,

Именуемая в дальнейшем «Работодатель» действующий на основании Положения и гражданин(ка) России \_\_\_\_\_,

Паспорт гражданина РФ \_\_\_\_\_, именуемый в дальнейшем «Работник»; именуемые в дальнейшем «Стороны» заключили настоящее Дополнительное соглашение о нижеследующем:

1. Дополнить служебный контракт № \_\_\_\_\_ от \_\_\_\_\_ в части обязанностей сотрудника следующим:

1.1. Работник обязуется:

1.1.1. Не разглашать сведения, составляющие персональные данные работников и контрагентов Администрации Макарьевского муниципального округа, сведения, составляющие персональные данные, полученные в ходе рабочего процесса от сторонних предприятий и организаций, и иную конфиденциальную информацию и сведения ограниченного доступа, доверенные или ставшие известными Работнику во время выполнения им договорных обязанностей;

1.1.2. Не сообщать устно или письменно, не передавать третьим лицам и не раскрывать публично сведения, указанные в п. 1.1.1, без соответствующего разрешения Работодателя;

1.1.3. Выполнять требования действующего законодательства, приказов, инструкций, положений и иных нормативных актов по обеспечению сохранности указанных в п. 1.1.1 сведений;

1.1.4. В случае попытки посторонних лиц получить сведения, указанные в п.1.1.1, немедленно сообщить об этом руководству;

1.1.5. Не использовать сведения, указанные в п.1.1.1, при осуществлении иной деятельности, которая в качестве конкурентного действия может нанести ущерб Работодателю;

1.1.6. Возместить причиненный Работодателю ущерб, если Работник виновен в разглашении сведений, указанных в п.1.1.1;

1.1.7. Незамедлительно сообщить руководству об утрате или недостатке носителей информации, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению сведений, указанных в п. 1.1.1;

1.1.8. При прекращении работ все материальные носители, содержащие сведения, указанные в п.1.1.1 (флеш-накопители, дискеты, компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), которые находились в распоряжении Работника в связи с выполнением им договорных обязанностей, передать руководству;

1.1.9. Использовать информационные ресурсы Работодателя и переданные Работодателем в распоряжение Работника технические средства хранения, обработки и передачи информации исключительно для выполнения им договорных обязанностей.

1.2. Работодатель обязуется до начала выполнения договорных обязанностей Работником довести до его сведения соответствующие положения документов по защите указанных в п.1.1.1 сведений, разглашение которых может нанести ущерб интересам Работодателя и нарушить данное Дополнительное соглашение.

1.3. Работодатель предоставляет Работнику необходимые условия для выполнения требований по охране указанных в п. 1.1.1 сведений, к которым допускается Работник.

1.4. Работник разрешает Работодателю производить контроль использования им информационных ресурсов Работодателя, а также использования им технических средств обработки, хранения и передачи информации, предоставленных Работодателем для выполнения Работником договорных обязанностей.

1.5. Работодатель оставляет за собой право, но не принимает каких-либо обязательств контролировать использование Работником информационных ресурсов, технических средств обработки, хранения и передачи информации, а также соблюдения Работником мер по охране указанных в п. 1.1.1 сведений.

1.6. Работник подтверждает, что не имеет никаких обязательств перед какими-либо физическими или юридическими лицами, которые входят в противоречие с настоящим Дополнительным соглашением или которые ограничивают его договорную деятельность в соответствии с настоящим Дополнительным соглашением.

1.7. Работнику известно, что разглашение указанных в п. 1.1.1 сведений, ставших ему известными в период выполнения им договорных обязанностей, может повлечь гражданско-правовую, либо уголовную ответственность, предусмотренную действующим законодательством.

2. Настоящее Дополнительное соглашение вступает в действие с момента подписания его Сторонами и сроком действия не ограничено.

С Перечнем персональных данных Администрации Макарьевского муниципального округа Костромской области, Положением о введении режима обработки персональных данных в администрации Макарьевского муниципального округа Костромской области и мерами ответственности за нарушение установленного режима обработки персональных данных, Положением по организации системы защиты персональных данных в администрации Макарьевского муниципального округа Костромской области, ознакомлен:

РАБОТНИК:

РАБОТОДАТЕЛЬ:

\_\_\_\_\_  
/подпись/ /фамилия и инициалы/

\_\_\_\_\_  
/подпись/ /фамилия и инициалы/

Адрес:

М.П.

Перечень  
информационных систем персональных данных, обрабатываемых  
в администрации Макарьевского муниципального округа

1. MS WORD
2. MS EXEL
3. 1С Предприятие: Бухгалтерский учет
4. 1С Предприятие; КАМИН: Расчет заработной платы
5. Контур-экстерн
6. СЭД
7. СУФД
8. СБЕРБАНК БИЗНЕСС ОНЛАЙН
9. СБИС

Перечень должностей администрации Макарьевского муниципального округа,  
замещение которых предусматривает осуществление обработки персональных  
данных либо осуществление доступа к персональным данным

1. Управляющий делами.
2. Начальник управления по обращениям граждан, информатизации и связи
3. Главный бухгалтер отдела бухгалтерского учета и отчетности.
4. Главный специалист отдела по мобилизационной работе, ГО и ЧС.
5. Секретарь руководителя
6. Секретарь административной комиссии.
7. Главный специалист - ответственный секретарь комиссии по делам несовершеннолетних и защите их прав.
8. Секретарь Жилищной комиссии