**Утверждаю**
**Директор ГАУПСО**
**«Редакция газеты «Среднеуральская волна»**

**_____/Маленьких С.В.**
**«16» января 2026 г.**
**Приказ 6-о от 16.01.2026**

# ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Государственного автономного учреждения печати Свердловской области «Редакция газеты «Среднеуральская волна»

Принято на основании:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
- Закон Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации»
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах»
- Постановление Пленума Верховного Суда РФ от 15.06.2010 № 16 «О практике применения судами закона «О СМИ»

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

### 1.1 Назначение и область действия

1.1.1. Настоящее Положение устанавливает требования к организации обработки и защиты персональных данных, обрабатываемых в государственном автономном учреждении печати Свердловской области «Редакция газеты «Среднеуральская волна» (далее – Учреждение), и определяет порядок деятельности Учреждения в этой области.

1.1.2. Положение разработано в целях обеспечения защиты прав и свобод физических лиц при обработке их персональных данных.

1.1.3. Настоящее Положение применяется ко всем персональным данным, обрабатываемым в Учреждении независимо от вида носителя (электронный или бумажный), способа обработки (автоматизированный или неавтоматизированный) и места хранения.

1.1.4. Область действия Положения распространяется на:

- сотрудников Учреждения;
- источников информации и лиц, упоминаемых в публикациях;
- подписчиков и читателей;
- контрагентов и деловых партнеров;
- иных физических лиц, персональные данные которых обрабатываются в Учреждении.

**1.2 Цели Положения**

1.2.1. Основными целями Положения являются:

- создание надежной системы защиты персональных данных от несанкционированного доступа и разглашения;
- обеспечение соответствия деятельности Учреждения требованиям законодательства Российской Федерации;
- определение ответственности должностных лиц за обеспечение защиты персональных данных;
- установление процедур и механизмов защиты персональных данных;
- минимизация рисков нарушения прав и свобод субъектов персональных данных;
- выполнение обязательств перед субъектами персональных данных.

**1.3 Нормативная база**

Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон о персональных данных);
- Законом Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации»;
- Приказом ФСТЭК России от 18.02.2013 № 21;
- Постановлением Правительства РФ от 01.11.2012 № 1119;
- нормативными правовыми актами Свердловской области;
- уставом Учреждения;
- иными локальными нормативными актами Учреждения.

## 2. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

### 2.1 Термины и определения

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

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

2.1.3. Оператор персональных данных – государственное, муниципальное или иное юридическое лицо, а также физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав обрабатываемых персональных данных и действия (операции), совершаемые с персональными данными.

2.1.4. Субъект персональных данных – физическое лицо, к которому относятся персональные данные.

2.1.5. Информационная система персональных данных (ИС ПД) – совокупность персональных данных, содержащихся в базах данных и обеспеченных техническими и организационными мерами, необходимыми для реализации установленных законом полномочий.

2.1.6. Согласие субъекта персональных данных – любое свободно данное специфичное и информированное выражение воли субъекта персональных данных, которым он подтверждает свое согласие на обработку персональных данных.

2.1.7. Защита персональных данных – деятельность по предотвращению нарушения прав, свобод и законных интересов субъектов персональных данных при обработке их персональных данных.

2.1.8. Безопасность персональных данных – состояние защищенности персональных данных от их незаконного обращения, случайного или умышленного уничтожения, модификации, блокирования, копирования, распространения и иных противоправных действий.

2.1.9. Инцидент безопасности персональных данных – события, отрицательно влияющие на безопасность персональных данных.

2.1.10. Категория персональных данных:

- общие персональные данные – фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес проживания, работа, образование, профессия;

- специальные персональные данные – информация о расовой, национальной принадлежности, политических взглядах, религиозных убеждениях, состоянии здоровья, интимной жизни, судимости;
- биометрические персональные данные – фотография, видеозапись, отпечатки пальцев, иные биометрические данные.

---

## 3. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

### 3.1 Виды обрабатываемых персональных данных

3.1.1. В Учреждении обрабатываются персональные данные следующих категорий:

**А. Персональные данные сотрудников:**

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные (серия, номер, дата выдачи, кем выдан, код подразделения);
- адрес места жительства;
- адрес регистрации по месту жительства;
- семейное положение и сведения о членах семьи;
- номер СНИЛС;
- номер ИНН;
- информация об образовании;
- информация о трудовой деятельности;
- информация о должности и профессии;
- размер заработной платы и иные выплаты;
- информация о социальных льготах;
- данные медицинского страхования;
- информация о командировках и отпусках;
- банковские реквизиты;
- номер контактного телефона;
- адрес электронной почты;
- сведения о повышении квалификации;
- иная информация, необходимая для трудовых отношений.
-

**Б. Персональные данные авторов, корреспондентов:**

- фамилия, имя, отчество;
- дата рождения (при необходимости);
- профессиональная специализация;
- квалификация и опыт;
- номер контактного телефона;
- адрес электронной почты;
- место работы (при наличии);
- фотография для публикации;
- сведения об авторских правах;
- иная информация, необходимая для издания и распространения материалов.

**В. Персональные данные лиц, упоминаемых в публикациях:**

- фамилия, имя, отчество;
- дата рождения;
- место жительства;
- место работы;
- должность;
- фотография;
- видеозапись;
- иная информация, необходимая для публикации в общественно значимых целях.

**Г. Персональные данные подписчиков и читателей:**

- фамилия, имя, отчество;
- адрес доставки подписки;
- номер контактного телефона;
- адрес электронной почты (при наличии);
- информация о способе оплаты (при наличии);
- реквизиты банковского счета (при подписке).

**Д. Персональные данные контрагентов и деловых партнеров:**

- фамилия, имя, отчество (для физических лиц);
- наименование организации и реквизиты;
- место нахождения;

- адрес электронной почты;
- номер контактного телефона;
- имя руководителя и иных должностных лиц;
- банковские реквизиты;
- иные сведения, необходимые для заключения и исполнения контрактов.

**3.2 Юридические основания для обработки персональных данных**

3.2.1. Обработка персональных данных в Учреждении осуществляется при наличии как минимум одного из следующих оснований:

- согласие субъекта персональных данных;
- необходимость обработки для исполнения договора, сторонами которого является субъект персональных данных;
- необходимость обработки для исполнения законодательства Российской Федерации;
- необходимость обработки для осуществления функций Учреждения, установленных законодательством;
- защита жизни, здоровья или иных жизненно важных интересов субъекта персональных данных;
- осуществление иных целей, не противоречащих целям, для которых были получены персональные данные.

3.2.2. **Для сотрудников Учреждения:**

- согласие на обработку персональных данных (оформляется при приеме на работу);
- необходимость для исполнения трудового договора;
- необходимость для исполнения законодательства Российской Федерации (налоговое, пенсионное, страховое право, трудовое право);
- защита жизни и здоровья работника;
- осуществление функций работодателя.

3.2.3. **Для авторов и корреспондентов:**

- согласие на обработку персональных данных (оформляется в авторском договоре);
- согласие на публикацию и распространение материалов (содержится в авторском договоре);
- необходимость для исполнения авторского договора;
- осуществление профессиональной деятельности журналиста в общественно значимых целях.

3.2.4. **Для лиц, упоминаемых в публикациях:**

- согласие субъекта на публикацию его персональных данных;
- распространение общественно значимой информации в целях информирования общества;
- осуществление законной профессиональной деятельности журналистов в соответствии с Законом РФ «О средствах массовой информации»;
- использование данных, обязательных к раскрытию по закону;
- при условии соблюдения принципа пропорциональности и недопущения нарушения прав и свобод субъекта персональных данных.

3.2.5. **Для подписчиков и читателей:**

- согласие на обработку персональных данных (оформляется при подписке);
- необходимость для исполнения договора подписки;
- исполнение требований налогового и иного законодательства.

3.2.6. **Для контрагентов и деловых партнеров:**

- согласие на обработку персональных данных;
- необходимость для исполнения договоров и контрактов;
- исполнение требований законодательства.

**3.3 Цели обработки персональных данных**

3.3.1. Персональные данные обрабатываются в следующих целях:

**А. Для сотрудников:**

- заключение, исполнение и расторжение трудовых договоров;
- ведение кадрового учета;
- организация труда и контроль трудовой дисциплины;
- расчет и выплата заработной платы, авансов и иных выплат;
- организация социального страхования;
- уплата налогов;
- организация охраны труда и безопасности;
- соблюдение требований законодательства;
- разрешение трудовых споров;
- связь с работниками в профессиональных целях.

**Б. Для авторов и корреспондентов:**

- заключение и исполнение авторских договоров;
- публикация и распространение материалов;
- организация платежей и расчетов;
- регистрация авторских прав;
- связь с авторами.

**В. Для лиц, упоминаемых в публикациях:**

- информирование общества об общественно значимых событиях и фактах;
- осуществление миссии СМИ как контроля общественного мнения;
- исполнение функции информирования граждан в соответствии с Законом РФ «О средствах массовой информации»;
- архивирование материалов.

**Г. Для подписчиков и читателей:**

- доставка газеты и распространение материалов;
- организация подписки;
- ведение рассылок и информирование о новых материалах;
- расчеты по оплате подписки.

**Д. Для контрагентов и деловых партнеров:**

- исполнение договоров и контрактов;
- организация платежей и расчетов;
- связь в деловых целях;
- исполнение требований законодательства.

**3.4 Сроки хранения персональных данных**

3.4.1. Сроки хранения персональных данных устанавливаются в зависимости от целей обработки:

**А. Персональные данные сотрудников:**

- в течение всего периода действия трудового договора;
- после расторжения трудового договора – в течение 50 лет (согласно требованиям законодательства о хранении трудовых книжек и кадровых документов);
- персональные данные в целях налогообложения и пенсионного обеспечения – в соответствии с требованиями налогового и пенсионного законодательства (минимум 6 лет после составления документа).

**Б. Персональные данные авторов:**

- в течение всего периода сотрудничества;
- после прекращения сотрудничества – в течение 50 лет (в целях документирования авторских прав и истории издания);
- данные, необходимые для бухгалтерского учета – в соответствии с требованиями налогового законодательства (минимум 6 лет).

**В. Персональные данные лиц, упоминаемых в публикациях:**

- в составе архива опубликованных материалов – в течение всего периода существования Учреждения (для целей архивирования и исторической документации);
- для служебных целей – в течение периода, необходимого для достижения целей обработки;
- может осуществляться удаление из активной базы данных при отсутствии правовых оснований для хранения, но материалы сохраняются в архиве.

**Г. Персональные данные подписчиков:**

- в течение периода действия подписки и в течение 3 лет после ее прекращения;
- данные, необходимые для учета платежей – в соответствии с требованиями налогового законодательства;
- согласно 152-ФЗ, может осуществляться удаление данных по требованию субъекта.

**Д. Персональные данные контрагентов:**

- в течение периода исполнения договора;
- после исполнения договора – в течение 6 лет (в соответствии с требованиями налогового законодательства);
- согласно 152-ФЗ, может осуществляться удаление данных по требованию субъекта при отсутствии иных оснований для хранения.

3.4.2. Все сроки хранения документируются в соответствующих локальных актах Учреждения.

---

## 4. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

### 4.1 Основные права

4.1.1. Субъект персональных данных имеет право:

- получать информацию, касающуюся обработки его персональных данных;
- требовать уточнения его персональных данных, их блокирования или удаления;

- возражать против обработки его персональных данных;
- требовать доступа к своим персональным данным;
- требовать информацию об источнике получения его персональных данных;
- требовать установления юридического лица, осуществляющего их обработку;
- требовать информацию о сроках хранения его персональных данных;
- требовать изложение позиции и возможность ее рассмотрения в соответствии с требованиями законодательства;
- судебную защиту своих прав;
- возмещение убытков и компенсацию морального вреда.

**4.2 Порядок реализации прав**

4.2.1. Субъект персональных данных реализует свои права путем подачи письменного заявления на адрес Учреждения:

**Адрес Учреждения:** 624071, Свердловская область, г. Среднеуральск, ул. Куйбышева,3

4.2.2. Заявление должно содержать:

- фамилию, имя, отчество заявителя;
- адрес проживания или электронной почты;
- содержание требования;
- скан или копию документа, удостоверяющего личность (копия паспорта);
- контактный телефон.

4.2.3. Заявление рассматривается в течение 30 дней с момента его получения.

4.2.4. При рассмотрении заявления Учреждение проверяет личность заявителя.

4.2.5. Ответ на заявление направляется субъекту персональных данных по адресу, указанному в заявлении, или по электронной почте.

4.2.6. В случае отказа в удовлетворении требования субъект персональных данных информируется об основаниях отказа и процедуре обжалования решения.

---

## 5. ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ ОПЕРАТОРА

**5.1 Обязательства Учреждения**

5.1.1. Учреждение в качестве оператора персональных данных обязано:

- обрабатывать персональные данные на основе принципов законности, добросовестности, справедливости и прозрачности;

- обеспечивать точность, полноту и актуальность персональных данных;
- осуществлять обработку персональных данных в целях, для которых они были получены;
- ограничивать объем обрабатываемых персональных данных;
- обеспечивать безопасность персональных данных;
- обеспечивать конфиденциальность персональных данных;
- предоставлять субъектам персональных данных информацию об обработке их персональных данных;
- уважать права и свободы субъектов персональных данных;
- осуществлять защиту персональных данных от несанкционированного доступа;
- вести реестр информационных систем персональных данных;
- уведомлять Роскомнадзор об инцидентах безопасности;
- осуществлять внутренний контроль соответствия требованиям законодательства;
- обучать работников требованиям защиты персональных данных;
- обеспечивать удаление или деструкцию персональных данных по завершении целей обработки;
- сотрудничать с органами государственной власти в сфере защиты персональных данных.

**5.2 Ответственность сотрудников Учреждения**

5.2.1. Сотрудники Учреждения, допустившие нарушения требований настоящего Положения, несут дисциплинарную ответственность в соответствии с Трудовым кодексом Российской Федерации, включая:

- замечание;
- выговор;
- увольнение.

5.2.2. За разглашение конфиденциальной информации, кроме того, может быть применена материальная ответственность.

**5.3 Административная и уголовная ответственность**

5.3.1. Нарушения требований законодательства о защите персональных данных могут влечь административную ответственность.

5.3.2. В особо тяжких случаях нарушитель может быть привлечен к уголовной ответственности в соответствии с Уголовным кодексом Российской Федерации.

## 6. СВЕДЕНИЯ О ПЕРСОНАЛЬНЫХ ДАННЫХ И СОГЛАСИЕ НА ОБРАБОТКУ

### 6.1 Информация для субъектов персональных данных

6.1.1. При сборе персональных данных субъект должен быть информирован о:

- наименовании оператора персональных данных;
- целях обработки персональных данных;
- составе обрабатываемых персональных данных;
- сроках обработки и хранения персональных данных;
- способах и месте обработки персональных данных;
- правах субъекта персональных данных;
- правах субъекта требовать доступа к своим персональным данным;
- праве возражать против обработки персональных данных;
- правах требовать уточнения, блокирования или удаления персональных данных;
- процедуре защиты прав субъектов персональных данных;
- контактной информации оператора.

6.1.2. Информация предоставляется в письменной или электронной форме.

### 6.2 Согласие на обработку персональных данных

6.2.1. **Форма согласия:**

- согласие оформляется в письменной форме;
- согласие может быть получено в электронной форме (через электронную почту, веб-форму на сайте);
- согласие должно быть свободно данным, специфичным и информированным;
- согласие содержит подпись субъекта персональных данных или иной способ подтверждения согласия.

6.2.2. **Содержание согласия:**

- наименование оператора;
- перечень обрабатываемых персональных данных;
- цель обработки;
- сроки обработки;
- иные условия обработки;
- информация о праве отозвать согласие.

6.2.3. **Согласие для различных категорий:**

**А. Для сотрудников:** Согласие на обработку персональных данных оформляется при приеме на работу как отдельный документ, приложение к трудовому договору или может быть включено в трудовой договор.

**Б. Для авторов:** Согласие включается в авторский договор.

**В. Для подписчиков:** Согласие оформляется при оформлении подписки.

**Г. Для лиц, упоминаемых в публикациях:** При возможности – предварительное согласие. В случаях, установленных Законом РФ «О СМИ», согласие не требуется (распространение общественно значимой информации).

### 6.3 Отзыв согласия

6.3.1. Субъект персональных данных может в любой момент отозвать свое согласие на обработку персональных данных посредством направления письменного заявления.

6.3.2. Отзыв согласия осуществляется посредством направления соответствующего заявления на адрес Учреждения.

6.3.3. После получения заявления об отзыве согласия Учреждение прекращает обработку персональных данных, кроме случаев, когда имеется иное законное основание для обработки.

---

## 7. БЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

### 7.1 Организационные меры защиты

7.1.1. Учреждение принимает следующие организационные меры по обеспечению безопасности персональных данных:

**А. Управление доступом:**

- определение должностных лиц и структурных подразделений, имеющих право доступа к персональным данным;
- ведение реестра лиц, имеющих доступ к персональным данным;
- разграничение прав доступа в соответствии с функциями;
- минимизация числа лиц, имеющих доступ к персональным данным;
- выдача индивидуальных идентификаторов пользователям;
- отзыв прав доступа при увольнении работника.

**Б. Обучение и инструктирование:**

- проведение обучения всех работников, имеющих доступ к персональным данным;

- обучение должно проводиться при приеме на работу и ежегодно;
- обучение включает требования 152-ФЗ, требования настоящего Положения, основные угрозы безопасности, методы защиты;
- проведение инструктажей по конфиденциальности;
- ведение реестра проведения обучения.

**В. Договоры и соглашения о конфиденциальности:**

- заключение с сотрудниками соглашений о конфиденциальности;
- включение положений о конфиденциальности в договоры с третьими лицами, имеющими доступ к персональным данным;
- обязательство третьих лиц (обработчиков, контрагентов) соблюдать требования законодательства о защите персональных данных.

**Г. Контроль и аудит:**

- регулярная проверка соответствия требованиям настоящего Положения;
- проведение внутреннего аудита не реже одного раза в год;
- документирование результатов аудита;
- анализ инцидентов и реализация корректирующих мер;
- уведомление руководства о выявленных нарушениях.

**Д. Процедуры при инцидентах:**

- немедленное выявление и фиксирование факта нарушения безопасности персональных данных;
- информирование руководства и ответственного за защиту персональных данных;
- проведение расследования;
- принятие мер по ограничению последствий;
- уведомление Роскомнадзора (при необходимости);
- уведомление субъектов персональных данных (при необходимости);
- документирование всех действий.

**7.2 Технические меры защиты**

7.2.1. Учреждение применяет следующие технические меры по обеспечению безопасности персональных данных:

**А. Для электронных данных:**

- использование защищенных каналов передачи данных (SSL, TLS);
- шифрование персональных данных при передаче и хранении;

- использование брандмауэров и систем обнаружения вторжений;
- антивирусная защита всех компьютеров;
- регулярное обновление операционных систем и программного обеспечения;
- резервное копирование данных;
- восстановление данных при их повреждении;
- логирование всех операций с персональными данными;
- контроль физического доступа к компьютерам и серверам;
- использование сильных паролей (минимум 8 символов, использование букв, цифр и специальных символов);
- двухфакторная аутентификация для критичных систем;
- использование VPN при удаленном доступе.

**Б. Для бумажных данных:**

- хранение в защищенных помещениях (шкафы, сейфы);
- ограничение физического доступа (ключи, охрана);
- уничтожение устаревших документов (сжигание, измельчение);
- надлежащее хранение документов, исключающее повреждение и утечку информации.

**В. Уничтожение данных:**

- перед уничтожением данные должны быть удалены способом, исключающим возможность их восстановления;
- для электронных данных – использование специализированного программного обеспечения для безвозвратного удаления;
- для бумажных документов – уничтожение должно быть документировано;
- ведение реестра уничтоженных данных.

**7.3 Информационные системы персональных данных**

7.3.1. Учреждение ведет реестр информационных систем персональных данных (ИС ПД), содержащий:

- наименование ИС;
- цель создания и функционирования;
- способ обработки данных (автоматизированный/неавтоматизированный);
- место расположения ИС;
- категории обрабатываемых персональных данных;

- источники получения данных;
- сроки хранения;
- лиц, ответственных за функционирование системы;
- список лиц, имеющих право доступа;
- принимаемые меры защиты;
- риски безопасности и угрозы.

7.3.2. ИС должны быть классифицированы по уровню защищенности в соответствии с Постановлением Правительства РФ № 1119.

---

## 8. УПРАВЛЕНИЕ СОГЛАСИЕМ И ИНФОРМИРОВАНИЕ СУБЪЕКТОВ

### 8.1 Сбор согласия

8.1.1. При сборе согласия Учреждение должна обеспечить:

- предоставление полной информации о целях и объеме обработки;
- свободный выбор и отсутствие принуждения;
- возможность отозвать согласие в любой момент;
- четкое и понятное формулирование условий.

### 8.2 Информирование об обработке

8.2.1. Учреждение информирует субъектов персональных данных об:

- наименовании оператора;
- целях обработки;
- составе персональных данных;
- сроках обработки;
- правах субъектов;
- способах реализации прав;
- процедурах защиты.

8.2.2. Информирование осуществляется:

- при первом сборе персональных данных;
- при обращении субъекта с соответствующим запросом;
- в соответствии с требованиями законодательства.

---

## 9. СПЕЦИФИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СМИ

### 9.1 Допустимость обработки без согласия

9.1.1. В соответствии с Законом РФ «О средствах массовой информации» и Федеральным законом о персональных данных, Учреждение может обрабатывать и публиковать персональные данные без согласия субъекта при соблюдении следующих условий:

**А. Распространение общественно значимой информации:**

- информация касается угроз демократическому правовому государству;
- информация касается угроз гражданскому обществу;
- информация касается угроз общественной безопасности;
- информация касается иных вопросов, имеющих общественное значение;
- объем и содержание персональных данных пропорциональны цели материала.

**Б. Осуществление законной профессиональной деятельности журналистов:**

- персональные данные необходимы для раскрытия информации;
- информация раскрывается в строгом соответствии с целями журналистского расследования;
- соблюдаются все требования о недопущении нарушения прав и свобод субъекта.

**В. Использование данных, обязательных к раскрытию:**

- персональные данные входят в перечень, обязательный к раскрытию по закону (например, сведения о государственных служащих);
- раскрытие осуществляется в соответствии с требованиями законодательства.

9.1.2. В любом случае должен соблюдаться принцип пропорциональности:

- содержание и объем персональных данных должны быть адекватны целям материала;
- недопустимо включение персональных данных, которые не необходимы для достижения информационной цели;
- недопустимо нарушение прав и свобод субъекта персональных данных.

### 9.2 Право на забвение в СМИ

9.2.1. Субъект персональных данных может требовать удаления его персональных данных из активного архива редакции при следующих условиях:

- данные больше не соответствуют целям их обработки;
- срок обработки истек;
- истек срок хранения в соответствии с настоящим Положением;

- отсутствуют иные основания для сохранения данных (архивное, историческое значение).

9.2.2. Однако персональные данные сохраняются в архиве для целей документирования истории, архивирования и исторической науки.

9.2.3. При удалении из активного архива осуществляется удаление или деанонимизация данных из поисковых систем и активных ресурсов.

### 9.3 Охрана чести, достоинства и репутации

9.3.1. При публикации материалов, содержащих персональные данные, Учреждение обязана:

- соблюдать требования редакционной этики;
- проверять точность опубликованной информации;
- избегать содержания, унижающего честь и достоинство человека;
- избегать распространения ложной информации;
- предоставлять возможность ответа публично обвиненному лицу;
- не разглашать информацию о частной жизни без необходимости;
- соблюдать правила журналистской деонтологии.

### 9.4 Контроль Роскомнадзора

9.4.1. Контроль за соблюдением требований настоящего Положения и законодательства о защите персональных данных осуществляет Роскомнадзор.

9.4.2. При выявлении нарушений Роскомнадзор:

- выносит предупреждение редакции;
- после двух предупреждений в течение года может обратиться в суд с иском о прекращении деятельности СМИ.

9.4.3. Учреждение обязана сотрудничать с органами власти и предоставлять запрашиваемую информацию.

---

## 10. УВЕДОМЛЕНИЕ ОБ ИНЦИДЕНТАХ

### 10.1 Порядок выявления и регистрации инцидентов

10.1.1. Инцидентом признается событие, которое привело или могло привести к:

- несанкционированному доступу к персональным данным;
- неправомерному изменению персональных данных;

- уничтожению персональных данных;
- разглашению персональных данных;
- нарушению конфиденциальности;
- нарушению целостности;
- нарушению доступности персональных данных.

10.1.2. При выявлении инцидента:

- лицо, выявившее инцидент, немедленно информирует руководителя подразделения и ответственного за защиту персональных данных;
- оформляется акт о случившемся инциденте;
- информация регистрируется в журнале инцидентов;
- проводится расследование причин и следствий инцидента;
- определяются меры по предотвращению подобных инцидентов.

**10.2 Уведомление Роскомнадзора**

10.2.1. Учреждение обязана уведомить Роскомнадзор об инцидентах при следующих условиях:

- произошла утечка персональных данных значительного объема;
- могут быть затронуты права и свободы значительного числа лиц;
- инцидент имеет серьезный характер.

10.2.2. Уведомление направляется не позднее, чем в течение одного рабочего дня с момента выявления инцидента.

**10.3 Уведомление субъектов персональных данных**

10.3.1. При возможности и необходимости Учреждение информирует субъектов персональных данных об инцидентах, которые могут:

- нарушить их права и свободы;
- причинить ущерб их интересам;
- содержать угрозу безопасности их персональных данных.

10.3.2. Уведомление включает информацию о:

- характере инцидента;
- затронутых персональных данных;
- возможных последствиях;
- принимаемых мерах по ограничению ущерба;

- способах защиты от возможного ущерба;
- контактной информации для получения дополнительной информации.

---

## 11. НАЗНАЧЕНИЕ ОТВЕТСТВЕННОГО ЛИЦА

### 11.1 Ответственный за защиту персональных данных

11.1.1. Приказом директора назначается ответственный за организацию обработки и защиты персональных данных (далее – ответственный).

11.1.2. Ответственный должен иметь:

- высшее образование;
- подготовку по вопросам защиты персональных данных.

11.1.3. Основные функции ответственного:

- организация обработки персональных данных в соответствии с требованиями законодательства;
- разработка и совершенствование локальных актов по защите персональных данных;
- организация обучения работников;
- осуществление внутреннего контроля соответствия;
- реагирование на инциденты безопасности;
- взаимодействие с органами власти;
- разработка мер по обеспечению безопасности;
- ведение реестра ИС персональных данных;
- составление отчетов для руководства и органов власти;
- консультирование работников по вопросам защиты персональных данных.

11.1.4. Ответственный подотчетен директору Учреждения.

---

## 12. ЛОКАЛЬНЫЕ АКТЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

### 12.1 Перечень локальных актов

12.1.1. Учреждение разрабатывает и принимает следующие локальные акты по защите персональных данных:

- Положение о защите персональных данных (настоящий документ);
- Перечень информационных систем персональных данных;

- Инструкция по обработке и защите персональных данных сотрудников;
- Инструкция по обработке и защите персональных данных подписчиков и читателей;
- Реестр лиц, имеющих доступ к персональным данным;
- Журнал инцидентов безопасности персональных данных;

### 12.2 Согласованность с общероссийским законодательством

12.2.1. Все локальные акты разрабатываются в соответствии с требованиями:

- Федерального закона о персональных данных;
- Закона РФ «О средствах массовой информации»;
- Приказа ФСТЭК России от 18.02.2013 № 21;
- Постановления Правительства РФ от 01.11.2012 № 1119;
- иными нормативными правовыми актами.

---

## 13. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ТРЕТЬИМИ ЛИЦАМИ

### 13.1 Передача персональных данных

13.1.1. Учреждение может передавать персональные данные третьим лицам (обработчикам, операторам) только при наличии:

- согласия субъекта персональных данных;
- иного юридического основания, предусмотренного законодательством;
- контракта между Учреждением и третьим лицом, содержащего обязательства по защите персональных данных.

13.1.2. Контракт должен содержать:

- перечень обрабатываемых персональных данных;
- цели обработки;
- сроки обработки;
- требования к безопасности и защите;
- обязательство третьего лица соблюдать требования законодательства;
- положения об ответственности;
- порядок уничтожения данных.

### 13.2 Разработчики и поставщики ИТ-решений

13.2.1. При работе с разработчиками программного обеспечения или поставщиками услуг Учреждение:

- заключает контракты, регламентирующие обработку персональных данных;
- требует соответствия требованиям ФСТЭК;
- проводит аудит систем и процедур защиты;
- требует наличия сертификации по информационной безопасности;
- обеспечивает соответствие требованиям законодательства.

---

## 14. ВНУТРЕННИЙ КОНТРОЛЬ И АУДИТ

### 14.1 Проведение внутреннего контроля

14.1.1. Учреждение регулярно проводит внутренний контроль соответствия требованиям законодательства о защите персональных данных.

14.1.2. Внутренний контроль проводится:

- не реже одного раза в год;
- при выявлении инцидентов безопасности;
- при изменении процессов обработки персональных данных;
- при внедрении новых ИС.

14.1.3. Контроль включает:

- проверку соответствия локальных актов требованиям законодательства;
- проверку правильности сбора и обработки персональных данных;
- проверку наличия согласия субъектов;
- проверку соответствия целей обработки;
- проверку сроков хранения;
- проверку безопасности и защиты;
- проверку ведения реестров и журналов;
- проверку обучения работников;
- проверку процедур при инцидентах.

14.1.4. По результатам контроля составляется акт, содержащий:

- дату проведения;
- проверяемые области и системы;
- выявленные нарушения;
- риски и уязвимости;

- рекомендации по устранению;
- сроки исправления.

### 14.2 Корректирующие меры

14.2.1. При выявлении нарушений Учреждение принимает корректирующие меры:

- разработка и утверждение плана исправления;
- назначение ответственных лиц;
- установление сроков;
- контроль выполнения;
- документирование результатов.

---

## 15. ПЕРЕХОДНЫЕ И ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

### 15.1 Вступление в силу

15.1.1. Настоящее Положение вступает в силу с момента его утверждения приказом директора Учреждения.

### 15.2 Сроки приведения в соответствие

15.2.1. Учреждение в течение 30 дней с момента утверждения Положения должна:

- разработать все необходимые локальные акты;
- внести изменения в существующие документы;
- назначить ответственного за защиту персональных данных;
- провести инвентаризацию информационных систем;
- разработать и согласовать реестр ИС персональных данных.

### 15.3 Ежегодное обновление

15.3.1. Положение подлежит ежегодному пересмотру на предмет соответствия изменениям в законодательстве и практике защиты персональных данных.

### 15.4 Отмена предыдущих документов

15.4.1. При вступлении в силу настоящего Положения отменяются все ранее действовавшие положения и инструкции по защите персональных данных в Учреждении.

### 15.5 Ответственность

15.5.1. За нарушение требований настоящего Положения в соответствии с законодательством наступает:

- дисциплинарная ответственность для работников;
- административная ответственность для Учреждения;
- уголовная ответственность в случаях, предусмотренных законом.

---

## 16. КОНТАКТНАЯ ИНФОРМАЦИЯ

**ГАУП СО «Среднеуральская волна»**

Адрес: 624071, Свердловская область, г. Среднеуральск, ул. Куйбышева,3

Телефон: 8(34368) 7-31-41

Электронная почта: 73113@sredneuralsk.info

Ответственный за защиту персональных данных: Загрядская Ольга Викторовна

Должность: главный бухгалтер

Телефон: 8(34368) 7-30-90

Электронная почта: 73113@sredneuralsk.info

---

## 17. ПРИЛОЖЕНИЯ

**Приложение 1. Бланк согласия на обработку персональных данных**

[Шаблон согласия должен быть разработан и утвержден отдельно]

**Приложение 2. Информация для субъектов персональных данных**

[Информационный листок должен быть разработан и утвержден отдельно]

**Приложение 3. Перечень информационных систем персональных данных**

[Реестр ИС должен быть разработан и актуализирован]

**Приложение 4. Инструкция по выявлению и регистрации инцидентов**

[Инструкция должна быть разработана и утверждена отдельно]

---

**Положение разработано:** директор Маленьких С.В.

**Согласовано:** главный бухгалтер Загрядская О.В.