КОМИТЕТ ПО ОБРАЗОВАНИЮ
АДМИНИСТРАЦИИ ВСЕВОЛОЖСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ЛЕНИНГРАДСКОЙ ОБЛАСТИ

Муниципальное учреждение
«Всеволожский районный методический центр»
(МУ «ВРМЦ»)

РАСПОРЯЖЕНИЕ

21.04.2025 № 234

г. Всеволожск

Об утверждении комплекта организационно-распорядительных документов по защите персональных данных в МУ «ВРМЦ»

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (с изменениями и дополнениями), ч. 1 ст. 89 ТК РФ, п. 8 ст. 86 ТК РФ, ст. 89 ТК РФ, постановлением Правительства Российской Федерации от 21 марта 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», с целью соблюдения требований законодательства Российской Федерации в части обработки и защиты персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»:

1. Утвердить и ввести в действие с 1 мая 2025 года нижеперечисленные организационно-распорядительные документы по защите персональных данных в МУ «ВРМЦ»:

1.1. Политика в отношении обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 1.

1.2. Положение об обработке персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 2.

1.3. Правила обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 3.

1.4. Положение по обеспечению безопасности персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 4.

1.5. Правила рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 5.

1.6. Правила внутреннего контроля обработки персональных данных на соответствие требованиям к их защите, утвержденным в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 6.

1.7. Инструкция ответственного за организацию обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 7.

1.8. Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 8.

1.9. Перечень лиц, имеющих доступ к персональными данным работников МУ «ВРМЦ» в связи с исполнением своих трудовых (служебных) обязанностей согласно Приложению № 9.

1.10. Инструкция пользователя информационных систем персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 10.

1.11. Порядок доступа в помещения, в которых размещены информационные системы персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» согласно Приложению № 11.

2. Куракиной Н.В., документоведу:

2.1. Довести до сведения работников МУ «ВРМЦ» настоящее распоряжение под подпись.

2.2. Обеспечить размещение организационно-распорядительных документов по защите персональных данных в МУ «ВРМЦ» согласно пункту 1 настоящего распоряжения в информационно-телекоммуникационной сети «Интернет» на официальном сайте МУ «ВРМЦ» https://rmc.vsevobr.ru/ в разделе «Сведения об учреждении» подраздел «Документы» https://rmc.vsevobr.ru/novosti/svedeniya-ob-obrazovatelnoj-organizatsii/dokumenty .

3. Признать утратившим силу распоряжение МУ «ВРМЦ» от 16 августа 2022 года № 298 «Об организации работы с персональными данными в МУ «ВРМЦ».

4. Контроль исполнения распоряжения оставляю за собой.

Директор Н.Н. Терешкова

Приложение № 1

УТВЕРЖДЕНА
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Политика в отношении обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения.

1.1. Настоящий документ определяет политику Муниципального учреждения «Всеволожский районный методический центр» (далее – Учреждение) в отношении обработки персональных данных (далее – Политика).

1.2. В настоящей Политике используются термины и определения, приведенные в таблице 1. Иные термины, применяемые в настоящей Политике, используются в значениях, определенных законодательством Российской Федерации иными нормативными правовыми актами, национальными стандартами в области обработки и защиты персональных данных.

Таблица 1 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Обезличивание персональных данных	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
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,	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»

Термин	Определение	Источник
	удаление, уничтожение персональных данных	
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Предоставление персональных данных	Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Распространение персональных данных	Действия, направленные на раскрытие персональных данных неопределенному кругу лиц	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем	ГОСТ Р 50739-95
Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

1.3. Учреждение осуществляет обработку персональных данных, а также определяет цели обработки персональных данных, состав персональных данных,

подлежащих обработке, действия (операции), совершаемые с персональными данными (далее – Оператор).

1.4. Настоящая Политика разработана на основании следующих нормативных правовых актов и рекомендаций:

- Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- рекомендации Федеральной службы в сфере связи, информационных технологий и массовых коммуникаций по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.5. Настоящая Политика, все дополнения и изменения к ней утверждаются распоряжением Учреждения.

1.6. Политика подлежит опубликованию на официальном сайте Учреждения.

1.7. Положения Политики распространяются на все отношения, связанные с обработкой персональных данных, осуществляемой в Учреждении, как с использованием средств автоматизации, так и без использования средств автоматизации.

1.8. Оператор ведет свою деятельность по адресу: 188640, Ленинградская область, Всеволожский район, г Всеволожск, Колтушское шоссе, д. 99. По данному адресу размещается исполнительный орган – директор.

База данных информации, содержащей персональные данные граждан Российской Федерации, находится по адресу: 188640, Ленинградская область, Всеволожский район, г. Всеволожск, Колтушское шоссе, д. 99.

1.9. Политика применяется ко всем работникам Учреждения.

1.10. Распоряжением Учреждения назначается ответственный за организацию обработки персональных данных (далее – ПДн).

2. Цели обработки персональных данных.

2.1. Целями обработки ПДн в Учреждении являются:

- осуществление хозяйственной деятельности, предусмотренной учредительными документами;
- соблюдение трудового законодательства и иных актов, содержащих нормы трудового права, включая учет труда и его оплаты, принятие управленческих и кадровых решений в отношении работников, контроль над трудовой дисциплиной;
- участие в гражданском, арбитражном, уголовном, административном процессах, а также исполнение судебных актов;
- ведение бухгалтерского учета, осуществление расчета и выплаты работникам причитающейся им заработной платы, компенсаций и премий, осуществление пенсионных и налоговых отчислений, а также расчет с подотчетными лицами;
- выпуск электронной-цифровой подписи, оформление доверенностей в рамках наделения работников и иных лиц специальными полномочиями для выполнения

возложенных на них трудовых функций и (или) представления интересов Учреждения;
- организация обучения, инструктажа, проверки знаний работников и иных лиц по охране труда и технике безопасности, а также проведение специальной оценки условий труда, проведение оценки профессиональных рисков на рабочем месте;
- организация и (или) осуществление обучения, повышения квалификации и проверки знаний для своих работников;
- организация ведения воинского учета работников - граждан Российской Федерации, создание необходимых условий для исполнения ими воинской обязанности;
- осуществление аттестации работников посредством оценки их деловых и личностных качеств, а также результатов их труда;
- осуществление расследования и учета несчастных случаев, происшедших с работниками при исполнении ими своих трудовых функций, а также в иных случаях, предусмотренных трудовым законодательством;
- публикация данных работников на сайте Учреждения, внутренних справочниках;
- осуществление надлежащего учета, хранения и уничтожения по истечении сроков хранения категорий материальных носителей информации;
- исполнение обязательств появившихся при заключении договорных отношений;
- замещение вакантных должностей соискателями, наиболее полно соответствующими должностным требованиям;
- принятие мер должной осмотрительности при взаимодействии с действительными и потенциальными контрагентами (агентами, партнерами, подрядчиками, поставщиками), включающее в себя оценку соответствующих юридических, финансовых, репутационных и иных рисков;
- связь с субъектами ПДн по вопросам, относящимся к предметам деятельности, а также взаимодействие с должностными/физическими лицами, представляющими юридические лица и индивидуальных предпринимателей, по вопросам сотрудничества с Учреждением;
- осуществление взаимных расчетов с контрагентами (клиентами, агентами, партнерами, подрядчиками, поставщиками);
- поставка товаров, выполнение работ и оказание услуг, в пользу Учреждения со стороны контрагентов (поставщиков), а также осуществление процедур закупок у указанных контрагентов и ведение деловых переговоров с указанными контрагентами;
- предоставление доступа к сервисам и информации, размещенной на сайте Учреждения.

3. Правовые основания обработки персональных данных.

3.1. Оператор обрабатывает ПДн на законной и справедливой основе для выполнения возложенных законодательством функций, полномочий и обязанностей, осуществления прав и законных интересов Оператора, работников Оператора и других физических лиц, ПДн которых обрабатываются в информационной системе Учреждения.

3.2. При обработке ПДн Оператор руководствуется следующими правовыми основаниями:
- Федеральный закон от 14.11.2002 № 161-ФЗ «О государственных и муниципальных унитарных предприятиях» (ст.28);

- Приказ Минфина России от 21 июля 2011 г. № 86н «Об утверждении порядка предоставления информации государственным (муниципальным) учреждением, ее размещения на официальном сайте и ведения указанного сайта»;
- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (п. 2 ст. 29);
- Постановление Правительства РФ от 20.10.2021 № 1802 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации, а также о признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации» (пп. 4, 10, 11);
- Конституция Российской Федерации (ст.ст. 23, 24);
- Трудовой кодекс Российской Федерации (ст.ст. 65, 66, 86-90, 166);
- Гражданский кодекс Российской Федерации (гл.гл. 39, 40, 52);
- Постановление Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты» (п. 2);
- Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством» (ч.4 ст.13);
- Устав Учреждения в действующей редакции;
- согласия субъектов персональных данных на обработку их персональных данных, а также договора, выгодоприобретателем или поручителем в которых являются субъекты персональных данных;
- Федеральный закон от 02.10.2007 г. № 229-ФЗ «Об исполнительном производстве» (гл. 11);
- Семейный кодекс Российской Федерации (гл. 17);
- Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ (п. 2 ст. 9);
- Налоговый кодекс Российской Федерации (ст.ст.226, 230, 24);
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (ст.ст.6, 9, 11);
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации» (ст.11);
- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» (ст. 38);
- Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (ст.ст. 14, 17);
- Федеральный закон от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда» (ч. 2 ст. 4, ст.ст. 7, 8);
- Постановление Правительства РФ от 24.12.2021 № 2464 «О порядке обучения по охране труда и проверки знания требований охраны труда» (пп. 86, 87, 90, 92);
- Федеральный закон «О воинской обязанности и военной службе» от 28.03.1998 № 53-ФЗ (п. 7 ст. 8);
- Федеральный закон «Об обороне» от 31.05.1996 № 61-ФЗ (подп. 6 п. 1 ст. 8);
- Приказ Минобороны от 22.11.2021 № 700;

- Постановление Правительства РФ от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»;
- Письмо ФНС России от 10 марта 2021 г. № БВ-4-7/3060@ (п. 15).

4. Объем и категории, обрабатываемых ПДн, категории субъектов ПДн.

4.1. В соответствии с целями обработки ПДн, указанными в п. 2 настоящей Политики, осуществляется обработка следующих категорий субъектов ПДн:

- действующие и уволенные работники (по ТК РФ), включая руководителя и лиц, состоящие в родстве;
- работники, не связанные трудовыми отношениями;
- соискатели вакантных мест;
- должностные лица контрагентов-организаций (ИП);
- физические лица - пользователи сайта Учреждения в информационно-телекоммуникационной сети «Интернет»;

4.2. Для каждой цели обработки персональных данных, обрабатываемых в Учреждении в Таблице 2 – «Объем и категории, обрабатываемых персональных данных, категории субъектов персональных данных» утверждаются объем, категории и перечни обрабатываемых персональных данных, категории субъектов персональных данных, обрабатываемых в информационных системах персональных данных, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей обработки или при наступлении законных оснований.

Таблица 2 – Объем и категории, обрабатываемых персональных данных, категории субъектов персональных данных

Цель обработки персональных данных №1	
Цель обработки ПД	Поиск и подбор лиц претендующих на замещение вакантных должностей (соискателей), включая следующие этапы: –поиск соискателей на замещение вакантных должностей; –информационное взаимодействие с соискателями; –оценка соответствия соискателей применимым требованиям, включая проверку знаний и способностей, проведение опросов; –проверка благонадежности соискателей, включающая в себя управление связанными с соискателями юридическими, репутационными и комплаенс (предотвращение и урегулирование конфликта интересов, противодействие коррупции) рисками, а также проверка полноты и достоверности предоставленных соискателями сведений; –принятие решения о приеме либо отказе в замещении вакантной должности (трудоустройстве);
Категории персональных данных	–фамилия, имя, отчество; –дата рождения; –место рождения; –пол; –информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); –вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи;

	–адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания; –номер контактного телефона, сведения о других способах связи; –сведения о трудовой деятельности, включая работу по совместительству, предпринимательскую и иную деятельность, военную службу; –сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование образовательного учреждения, год окончания, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании); –сведения об ученой степени, ученом звании (когда присвоено, номера дипломов, аттестатов); –сведения о владении иностранными языками, степень владения; –информация о наличии или отсутствии судимости; –государственные награды, иные награды и знаки отличия; –сведения о профессиональной переподготовке и (или) повышении квалификации;
Категории субъектов, персональные данные которых обрабатываются	Соискатели вакантных мест
Правовое основание обработки персональных данных	Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных
Перечень действий	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение
Способы обработки	смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет;
Цель обработки персональных данных №2	
Цель обработки ПД	Обеспечение соблюдения требований трудового законодательства при управлении персоналом, включая следующие этапы: –оформление приема на работу; –ознакомление и адаптация к трудовой деятельности и социальной среде (онбординг); –выполнение трудовой функции и исполнение должностных (служебных) обязанностей; –ведение кадрового и воинского учета; –принятие управленческих и кадровых решений, обеспечение развития трудовой карьеры и продвижение по службе; –оформление командировок и иных служебных поездок; –предоставление отпуска и дополнительных дней отдыха (отгул); –организация режима дистанционной (удаленной) работы; –управление трудовыми ресурсами, планирование должностной преемственности;

	–планирование работы персонала и управление производительностью труда, мониторинг и контроль количества и качества выполняемой работы, а также рационального использования рабочего времени, проверка и оценка исполнения должностных обязанностей; –рассмотрение и разрешение трудовых споров, конфликтных ситуаций и иных разногласий в контексте трудовых отношений;
Категории персональных данных	–фамилия, имя, отчество; –предыдущие фамилия, имя, отчество, если изменялись; –пол; –дата рождения; –место рождения; –информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); –налоговый статус; –вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи; –адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания; –номер контактного телефона, сведения о других способах связи; –информация о наличии или отсутствии судимости; –реквизиты документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета; –идентификационный номер налогоплательщика; –реквизиты страхового медицинского полиса обязательного медицинского страхования; –реквизиты свидетельства государственной регистрации актов гражданского состояния; –сведения о семейном положении, составе семьи: степень родства, фамилии, имена, отчества (при наличии); –сведения о трудовой деятельности, включая работу по совместительству, предпринимательскую и иную деятельность, военную службу; –отношение к воинской обязанности, сведения о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документов воинского учета, наименование органа, выдавшего его); –информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; –наименование должности; –наименование структурного подразделения; –наименование и адрес текущего места трудоустройства; –реквизиты (сведения о дате заключения и номер) трудового договора; –дата приема на работу; –дата вступления в должность; –сведения о факте и дате прекращения трудового договора;

	–реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) трудовой книжки; –наименование профессии; –сведения о трудовом стаже; –сведения о месте и дате направления в командировку; –ведения о факте, периоде и продолжительности нахождения в командировке; –сведения о сумме произведенных командировочных расходов;
Категории субъектов, персональные данные которых обрабатываются	Работники Уволенные работники
Правовое основание обработки персональных данных	–Согласие субъекта персональных данных на обработку его персональных данных; –Конституция Российской Федерации (ст.ст. 23, 24); –Постановление Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты» (п. 2); –Федеральный закон «О воинской обязанности и военной службе» от 28.03.1998 N 53-ФЗ (п. 7 ст. 8); –Федеральный закон «Об обороне» от 31.05.1996 № 61-ФЗ (подп. 6 п. 1 ст. 8); –Приказ Минобороны от 22.11.2021 № 700; –Постановление Правительства РФ от 27.11.2006 N 719 «Об утверждении Положения о воинском учете»; –Гражданский кодекс Российской Федерации (гл.гл. 39, 52); –Трудовой кодекс Российской Федерации (ст.ст. 86-90, 166).
Перечень действий	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение
Способы обработки	смешанная; с передачей по внутренней сети юридического лица; без передачи по сети Интернет;
Цель обработки персональных данных №3	
Цель обработки ПД	Осуществление ведения бухгалтерского и налогового учета в отношении персонала, включая следующие этапы: –расчет и выплата заработной платы, доплат, премий, бонусов, пособий, возмещений по понесенным расходам, компенсаций, материальной помощи, вознаграждений за служебные результаты интеллектуальной деятельности и осуществление прочих выплат, а также предоставление налоговых вычетов; –расчет и осуществление пенсионных и налоговых отчислений, удержаний из заработной платы и иных доходов в предусмотренных законом случаях, а также расчет с подотчетными лицами; –ведение бухгалтерского и налогового учета в отношении персонала;
Категории персональных	–фамилия, имя, отчество;

данных	–предыдущие фамилия, имя, отчество, если изменялись; –пол; –дата рождения; –место рождения; –информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); –образец подписи; –налоговый статус; –вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи; –адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания; –номер контактного телефона, сведения о других способах связи; –информация о наличии или отсутствии судимости; –реквизиты документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета; –идентификационный номер налогоплательщика; –реквизиты страхового медицинского полиса обязательного медицинского страхования; –реквизиты свидетельства государственной регистрации актов гражданского состояния; –сведения о семейном положении, составе семьи: степень родства, фамилии, имена, отчества (при наличии); –сведения о трудовой деятельности, включая работу по совместительству, предпринимательскую и иную деятельность, военную службу; –отношение к воинской обязанности, сведения о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документов воинского учета, наименование органа, выдавшего его); –информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; –сведения о начисленной и удержанной заработной плате; –сведения о начисленных и уплаченных страховых взносах; –сведения о премиях; –наименование должности; –наименование структурного подразделения; –наименование и адрес текущего места трудоустройства; –реквизиты (сведения о дате заключения и номер) трудового договора; –дата приема на работу; –дата вступления в должность; –сведения о факте и дате прекращения трудового договора; –реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) трудовой книжки; –наименование профессии; –сведения о трудовом стаже; –сведения о месте и дате направления в командировку;

	–ведения о факте, периоде и продолжительности нахождения в командировке; –сведения о сумме произведенных командировочных расходов.
Категории субъектов, персональные данные которых обрабатываются	Работники
Правовое основание обработки персональных данных	–Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством» (ч.4 ст.13); –Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ (п. 2 ст. 9); –Налоговый кодекс Российской Федерации (ст.ст.226, 230, 24); –Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (ст.ст.6, 9, 11); –Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации» (ст.11); –Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» (ст. 38); –Семейный кодекс Российской Федерации (гл. 17).
Перечень действий	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение
Способы обработки	смешанная; с передачей по внутренней сети юридического лица; без передачи по сети Интернет;
Цель обработки персональных данных №4	
Цель обработки ПД	Осуществление мер, направленных на обеспечение безопасности труда, повышение продуктивности и развития персонала, включая следующие этапы: –поддержание эффективного информационного и организационного взаимодействия между работодателем и персоналом; –организация и (или) проведение обучения различного характера (включая инструктаж), повышения квалификации, профессиональной (пере) \ подготовки, проверка знаний и способностей, проведение интервью (опросов) служебного и иного характера; –обеспечение, контроль, обучение (включая инструктаж), стажировка и проверка знаний в отношении охраны труда, техники безопасности, пожарной безопасности, гражданской обороны и защиты от чрезвычайных (аварийных) ситуаций; –проведение специальной оценки условий труда (СОУТ); –расследование, оформление (рассмотрение), учет, оповещение в отношении микроповреждений (микротравм),

	несчастных случаев и профессиональных заболеваний;
Категории персональных данных	–фамилия, имя, отчество; –предыдущие фамилия, имя, отчество, если изменялись; –пол; –дата рождения; –место рождения; –информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); –образец подписи; –налоговый статус; –вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи; –адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания; –номер контактного телефона, сведения о других способах связи; –информация о наличии или отсутствии судимости; –реквизиты документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета; –идентификационный номер налогоплательщика; –реквизиты страхового медицинского полиса обязательного медицинского страхования; –реквизиты свидетельства государственной регистрации актов гражданского состояния; –сведения о семейном положении, составе семьи: степень родства, фамилии, имена, отчества (при наличии); –сведения о трудовой деятельности, включая работу по совместительству, предпринимательскую и иную деятельность, военную службу; –отношение к воинской обязанности, сведения о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документов воинского учета, наименование органа, выдавшего его); –информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; –наименование должности; –наименование структурного подразделения; –наименование и адрес текущего места трудоустройства; –реквизиты (сведения о дате заключения и номер) трудового договора; дата приема на работу; –дата вступления в должность; –сведения о факте и дате прекращения трудового договора; –реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) трудовой книжки; –наименование профессии; –сведения о трудовом стаже; –сведения о месте и дате направления в командировку; –ведения о факте, периоде и продолжительности нахождения в командировке;

	–сведения о сумме произведенных командировочных расходов.
Категории субъектов, персональные данные которых обрабатываются	Работники
Правовое основание обработки персональных данных	–Федеральный закон от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда» (ч. 2 ст. 4, ст.ст. 7, 8); –Постановление Правительства РФ от 24.12.2021 № 2464 «О порядке обучения по охране труда и проверки знания требований охраны труда» (пп. 86, 87, 90, 92); –ТК РФ ст. 218; –Федеральный закон от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения» (ст.11, ст.34, п.7).
Перечень действий	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение
Способы обработки	смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет;
Цель обработки персональных данных №5	
Цель обработки ПД	Информационно-технологическое обеспечение безопасности деятельности организации и персонала, включая: –обеспечение сохранности имущества и защиты физических лиц от противоправных деяний (посягательств);
Категории персональных данных	–фамилия, имя, отчество; –вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи; –адрес и дата регистрации по месту жительства (месту пребывания).
Категории субъектов, персональные данные которых обрабатываются	Работники
Правовое основание обработки персональных данных	ТК РФ (ст. 238)
Перечень действий	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение
Способы обработки	смешанная; с передачей по внутренней сети юридического лица; без передачи по сети Интернет;
Цель обработки персональных данных №6	
Цель обработки ПД	Обеспечение правомерности и эффективности, при осуществлении хозяйственной деятельности, включая следующие этапы: –обеспечение эффективности и устойчивости (непрерывности) деятельности, организация и управление

	деятельностью и активами (имуществом), стратегическое и бюджетное планирование, управление проектами, ведение необходимой отчетности, управление сделками по реорганизации, слиянию, поглощению, ликвидации или отчуждению активов, координация и взаимодействие с аффилированными и иными связанными лицами; –осуществление прав, выполнение обязанностей и соблюдение запретов, предусмотренных любыми применимыми нормами, включая нормы законодательства, локальных актов, международных, национальных, отраслевых, профессиональных стандартов; защита прав и законных интересов, включая использование всех доступных средств правовой защиты и возможностей по ограничению объема наносимого вреда, а также делегирование (оформление) полномочий на представление интересов; участие во внесудебном и судебном урегулировании споров, исполнение судебных актов, содействие в отправлении правосудия;
Категории персональных данных	–фамилия, имя, отчество; –вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи; –адрес и дата регистрации по месту жительства (месту пребывания); –номер контактного телефона, сведения о других способах связи; –наименование должности;
Категории субъектов, персональные данные которых обрабатываются	Работники Контрагенты Клиенты
Правовое основание обработки персональных данных	Обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах; Федеральный закон от 02.10.2007 г. № 229-ФЗ «Об исполнительном производстве» (гл. 11).
Перечень действий	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение
Способы обработки	смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет;
Цель обработки персональных данных № 7	
Цель обработки ПД	Осуществление хозяйственной деятельности, предусмотренной учредительными (регистрационными) документами, а также ее сопровождение, включая следующие этапы: –организация и ведение делопроизводства, обеспечение внутреннего и внешнего документооборота (в письменной и электронной форме), ведение юридически значимой переписки (в письменной и электронной форме);

	–осуществление надлежащих учета, хранения и уничтожения отдельных категорий материальных носителей информации; –ведение договорной работы, в том числе заключение, исполнение, изменение и прекращение договоров и соглашений с контрагентами; –осуществление финансовых расчетов с лицами, не являющимися персоналом, ведение соответствующего бухгалтерского и налогового учета, независимая проверка бухгалтерской (финансовой) отчетности; –организация, осуществление и управление эффективностью процедур закупок продукции (товаров, работ, услуг) у контрагентов; –принятие мер должной осмотрительности в отношении потенциальных и действующих контрагентов, включающее в себя управление связанными с контрагентами финансовыми, коммерческими, юридическими, регуляторными, операционными, контрактными, репутационными и иными рисками; –осуществление информационного и (или) организационного взаимодействия со всеми заинтересованными лицами (включая информационное обеспечение, направление информационных сообщений, обработку поступающих обращений и информационных материалов любого характера и подготовку ответа на них, предоставление эффективной помержки при возникновении у заинтересованных лиц различных проблем или ситуаций), а также управление качеством и эффективностью такого взаимодействия (обслуживания); –поиск, определение и анализ потенциально заинтересованных в сотрудничестве лиц, установление и поддержание делового общения с заинтересованными лицами, участие в процедурах закупок потенциальных и действующих контрагентов;
Категории персональных данных	–фамилия, имя, отчество; –дата рождения; –место рождения; –вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи; –адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания; –номер контактного телефона, сведения о других способах связи;
Категории субъектов, персональные данные которых обрабатываются	Работники Контрагенты Представители контрагентов Выгодоприобретатели по договорам Клиенты
Правовое основание обработки персональных данных	–Письмо ФНС России от 10 марта 2021 г. № БВ-4-7/3060@ (п. 15); –Федеральный закон от 06.04.2011 г. № 63-ФЗ

	«Об электронной подписи» (ст.ст. 14, 17);
Перечень действий	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение
Способы обработки	смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет;

5. Принципы и условия обработки персональных данных.

5.1. При обработке ПДн в Учреждении соблюдаются следующие принципы:

- обработка ПДн осуществляется на законной и справедливой основе;
- обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка ПДн, несовместимая с целями сбора ПДн;
- не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только ПДн, которые отвечают целям их обработки;
- содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки;
- обрабатываемые ПДн не являются избыточными по отношению к заявленным целях их обработки;
- при обработке ПДн обеспечивается точность ПДн, их достаточность и в необходимых случаях актуальность по отношению к целям обработки ПДн;
- принимаются необходимые меры по удалению или уточнению неполных, или неточных ПДн;
- хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн; обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

5.2. В Учреждении осуществляется как автоматизированная обработка ПДн, так и без использования средств автоматизации.

Совокупность операций обработки ПДн в Учреждении включает:

- сбор,
- запись,
- систематизация,
- накопление,
- хранение,
- уточнение (обновление, изменение),
- извлечение,
- использование,
- передача (предоставление, доступ),
- блокирование,
- удаление,

– уничтожение,
– распространение.

5.3. При сборе ПДн Учреждение обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных с использованием баз данных, находящихся на территории Российской Федерации.

5.4. Учреждение осуществляет передачу ПДн третьим лицам в соответствии с требованиями законодательства Российской Федерации в области обработки и защиты ПДн.

Учреждение в ходе своей деятельности вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

При этом обязательным условием предоставления и/или поручения обработки ПДн другому лицу является обязанность сторон по соблюдению конфиденциальности и обеспечению безопасности ПДн при их обработке.

В поручении Учреждения определяется перечень ПДн, перечень действий (операций) с ПДн, которые будут осуществляться лицом, осуществляющим обработку ПДн, цели их обработки, а также устанавливается обязанность такого лица соблюдать конфиденциальность ПДн, требования, частью 5 статьи 18 и статьей 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), обязанность по запросу Учреждения в течение срока действия поручения Учреждения, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Учреждения требований по обеспечению безопасности и защиты ПДн при их обработке в соответствии с Федеральным законом.

5.5. В случаях, когда Учреждение поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Учреждение.

5.6. Прекращение обработки ПДн осуществляется при наступлении одного из следующих условий:
– ликвидация, реорганизация, прекращение деятельности Учреждения;
– достижение целей обработки ПДн и максимальных сроков хранения;
– утрата необходимости в достижении целей обработки;
– предоставление субъектом ПДн или его законным представителем сведений, подтверждающих, что ПДн являются незаконно полученными для заявленной цели обработки;
– невозможность обеспечения правомерности обработки ПДн;
– отзыв субъектом ПДн согласия на обработку ПДн.

5.7. Трансграничная передача ПДн Учреждением не осуществляется.

5.8. В Учреждении обеспечивается конфиденциальность ПДн. Работники Учреждения, получившие доступ к ПДн, не раскрывают третьим лицам и не распространяют ПДН без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

5.9. В Учреждении допускается обработка общедоступных ПДн.

5.10. Обработка иных категорий ПДн осуществляется Учреждением с соблюдением следующих условий:

- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

6. Реализация мер обеспечения безопасности персональных данных, принимаемых в Учреждении.

6.1. Учреждение принимает или обеспечивает принятие необходимых и достаточных правовых, организационных и технических мер для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

К таким мерам в Учреждении относятся:

- назначение лица, ответственного за организацию обработки ПДн;
- издание локальных актов по вопросам обработки ПДн, определяющих для каждой цели обработки ПДн категории и перечень обрабатываемых ПДн, категорий субъектов, ПДн которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявления нарушений законодательства Российской Федерации в области обработки и защиты ПДн, устранение последствий таких нарушений;
- осуществление внутреннего контроля соответствия обработки ПДн законодательству Российской Федерации о персональных данных, требованиям к защите ПДн, внутренним документам Учреждения в области обработки и защиты ПДн;
- оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- ознакомление работников Учреждения с положениями законодательства Российской Федерации о ПДн, внутренними документами Учреждения по вопросам обработки ПДн, требованиями к защите ПДн;
- применение или обеспечение применения правовых, организационных и технических мер по обеспечению безопасности ПДн в соответствии со ст.19 Федерального закона «О персональных данных», в частности:
  - определение угроз безопасности ПДн при их обработке в информационных системах ПДн Учреждения;
  - реализация технических и организационных мер по защите ПДн, обрабатываемых в информационных системах ПДн Учреждения, на основе требований, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и требований приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при

их обработке в информационных системах персональных данных» выработанных по результатам:

- определения категорий ПДн, обрабатываемых в информационных системах ПДн Учреждения;
- определения уровня защищенности ПДн при их обработке в информационных системах ПДн на основе анализа актуальных угроз безопасности ПДн и возможного ущерба субъектам ПДн при реализации угроз безопасности ПДн;
- организация режима обеспечения безопасности помещений, в которых размещены информационные системы ПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях, не имеющих права доступа в эти помещения;

- обеспечение учета и сохранности машинных носителей ПДн;
- организация доступа к ПДн, обрабатываемым в информационных системах ПДн;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;
- реализация антивирусного мониторинга и детектирования;
- применение межсетевых защитных (фильтрующих) экранов;
- своевременное установление обновлений используемого программного обеспечения информационных систем ПДн и средств защиты информации;
- организация защиты технических средств информационных систем ПДн.

6.2. В Учреждении в установленном порядке обеспечивается взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн.

7. Обработка персональных данных, осуществляемая без использования средств автоматизации

7.1. ПДн при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее – материальные носители), в специальных разделах или на полях форм (бланков).

7.2. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн используется отдельный материальный носитель.

7.3. Лица, осуществляющие обработку ПДн без использования средств автоматизации (в том числе работники Учреждения или лица, осуществляющие такую обработку по договору с Учреждением) проинформированы о факте обработки ими ПДн, обработка которых осуществляется Учреждением без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных

нормативными правовыми актами Российской Федерации, а также локальными правовыми актами Учреждения.

7.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), соблюдаются следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Учреждения, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых Учреждением способов обработки ПДн;
- типовая форма предусматривает поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку ПДн;
- типовая форма составляется таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- типовая форма исключает объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

7.5. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, принимаются меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

7.6. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Положения, предусмотренные в настоящем пункте и пункте 7.5. настоящей Политики применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе ПДн и информации, не являющейся ПДн.

7.7. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями

материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

7.8. Меры по обеспечению безопасности ПДн при их обработке, осуществляемой без использования средств автоматизации:

- обработка ПДн, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории ПДн можно определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;
- обеспечивается раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях;
- при хранении материальных носителей соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются распоряжением Учреждения.

8. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным.

8.1. Права субъектов ПДн:

8.1.1. Право субъекта ПДн на доступ к его ПДн:

1) Субъект ПДн имеет право на получение информации (далее – запрашиваемая субъектом информация), касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Учреждением;
- правовые основания и цели обработки ПДн;
- цели и применяемые Учреждением способы обработки ПДн;
- наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения Оператором обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

2) Субъект ПДн имеет право на получение запрашиваемой субъектом информации, за исключением случаев, когда доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

3) Субъект ПДн вправе требовать от Учреждения уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4) Запрашиваемая субъектом информация должна быть предоставлена субъекту ПДн от Учреждения в доступной форме, и в ней не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

5) Запрашиваемая информация предоставляется субъекту ПДн или его представителю Учреждением **в течение 10 рабочих дней** с момента обращения либо при получении запроса субъекта ПДн или его представителя.

Указанный срок может быть продлен, но не более чем на **5 рабочих дней** в случае направления Учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Учреждением, подпись субъекта ПДн или его представителя (далее – необходимая для запроса информация).

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Учреждение предоставляет сведения субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение или запрос, если иное не указано в обращении или запросе.

6) В случае если запрашиваемая субъектом информация, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения запрашиваемой субъектом информации и ознакомления с такими ПДн **не ранее чем через 30 дней** после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

7) Субъект ПДн вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения запрашиваемой субъектом информации, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в подпункте 6 пункта 8.1.1. настоящей Политики, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос наряду с необходимой для запроса информацией должен содержать обоснование направления повторного запроса.

8) Учреждение вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям повторного запроса.

Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

8.1.2. Право на обжалование действий или бездействия Учреждения:

1) Если субъект ПДн считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Учреждения в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

2) Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8.1.3. Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации Учреждением не осуществляется.

8.2. Обязанности Оператора:

8.2.1. Обязанности Оператора при сборе ПДн:

1) При сборе ПДн Учреждение предоставляет субъекту ПДн по его просьбе запрашиваемую информацию, касающуюся обработки его ПДн в соответствии с частью 7 статьи 14 Федерального закона «О персональных данных».

2) Если предоставление ПДн и (или) получение Учреждением согласия на обработку ПДн являются обязательными в соответствии с федеральным законом, Учреждение разъясняет субъекту ПДн юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку.

3) Если ПДн получены не от субъекта ПДн, Учреждение до начала обработки таких ПДн предоставляет субъекту ПДн следующую информацию (далее – информация, сообщаемая при получении ПДн не от субъекта персональных данных):

- наименование либо фамилия, имя, отчество и адрес Учреждения;
- цель обработки ПДн и ее правовое основание;
- перечень ПДн;
- предполагаемые пользователи ПДн;
- установленные Федеральным законом «О персональных данных» права субъекта ПДн;
- источник получения ПДн.

4) Учреждение не предоставляет субъекту информацию, сообщаемую при получении ПДн не от субъекта персональных данных, в случаях, если:

- субъект ПДн уведомлен об осуществлении обработки его ПДн Учреждением;
- ПДн получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

- обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 от 27.06.2006 № 152-ФЗ «О персональных данных»;
- Учреждение осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;
- предоставление субъекту ПДн информации, сообщаемой при получении ПДн не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

8.2.2. Обязанности Оператора при обращении к нему субъекта ПДн либо при получении запроса субъекта ПДн или его представителя, а также уполномоченного органа по защите прав субъектов ПДн:

1) Учреждение сообщает в установленном порядке субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставляет возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо **в течение 10 рабочих дней** с даты получения запроса субъекта ПДн или его представителя.

Указанный срок может быть продлен, но не более чем на **5 рабочих дней** в случае направления Учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2) В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя Учреждение дает в письменной форме мотивированный ответ в срок, **не превышающий 10 рабочих дней** со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

Указанный срок может быть продлен, но не более чем на **5 рабочих дней** в случае направления Учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3) Учреждение предоставляет безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн.

В срок, **не превышающий 7 рабочих дней** со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения.

В срок, **не превышающий 7 рабочих дней** со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Учреждение уничтожает такие ПДн.

Учреждение уведомляет субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

4) Учреждение сообщает в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию **в течение 10 рабочих дней** с даты получения такого запроса.

Указанный срок может быть продлен, но не более чем на **5 рабочих дней** в случае направления Учреждением в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

8.2.3. Обязанности Оператора по устранению нарушений законодательства, допущенных при обработке ПДн, по уточнению, блокированию и уничтожению ПДн:

1) В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн Учреждение осуществляет блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Учреждение осуществляет блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

2) В случае подтверждения факта неточности ПДн Учреждением на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов уточняет ПДн либо обеспечивает их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждением) **в течение 7 рабочих дней** со дня представления таких сведений и снимает блокирование ПДн.

3) В случае выявления неправомерной обработки ПДн, осуществляемой Учреждением или лицом, действующим по поручению Учреждения в срок, **не превышающий 3 рабочих дней** с даты этого выявления, прекращает неправомерную обработку ПДн или обеспечивает прекращение неправомерной обработки ПДн лицом, действующим по поручению Учреждения. В случае если обеспечить правомерность обработки ПДн невозможно, Учреждение в срок, **не превышающий 10 рабочих дней** с даты выявления неправомерной обработки ПДн, уничтожает такие ПДн или обеспечивает их уничтожение.

Об устранении допущенных нарушений или об уничтожении ПДн Учреждение уведомляет субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

4) В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, Учреждение обязано с момента выявления такого инцидента

оператором, уполномоченным органом по защите прав субъектов ПДн или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов ПДн:

- **в течение 24 часов** о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Учреждением на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом;
- **в течение 72 часов** о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5) В случае достижения цели обработки ПДн Учреждение прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждение) и уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждением) в срок, **не превышающий 30 дней** с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

6) В случае отзыва субъектом ПДн согласия на обработку его ПДн Учреждение прекращает их обработку или обеспечивает прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждение) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, **не превышающий 30 дней** с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

7) В случае обращения субъекта ПДн в Учреждение с требованием о прекращении обработки ПДн оператор обязан в срок, **не превышающий 10 рабочих дней** с даты получения Оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку ПДн), за исключением случаев, предусмотренных Федеральным законом «О персональных данных».

Указанный срок может быть продлен, но не более чем на **5 рабочих дней** в случае направления оператором в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

8) В случае отсутствия возможности уничтожения ПДн в течение указанного срока, Учреждение блокирует такие ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение ПДн в срок **не более чем 6 месяцев**, если иной срок не установлен федеральными законами.

8.3. Правила рассмотрения запросов субъектов персональных данных или их представителей в Учреждение, а также формы рассмотрения соответствующих запросов субъектов персональных данных или их представителей устанавливаются распоряжением Учреждения.

9. Ответственность

9.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут ответственность, предусмотренную законодательством Российской Федерации.

9.2. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, установленных Федеральным законом «О персональных данных», а также требований к защите ПДн, установленных в соответствии с Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

10. Срок действия.

10.1. Политика утверждается на неопределенный срок.

10.2. В настоящую Политику могут вноситься изменения и дополнения, утверждаемые распоряжением Учреждения.

Приложение № 2

УТВЕРЖДЕНА
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Положение

об обработке персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1.1. Настоящее Положение об обработке персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными федеральными и региональными нормативными актами в сфере защиты персональных данных, Политикой обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр».

1.2. Положение определяет порядок работы с персональными данными в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) соискателей на вакантные должности, работников, в том числе бывших, их родственников, а также гарантии конфиденциальности личной информации, которую соискатели и работники предоставляют Учреждению.

1.3. Целью Положения является защита персональных данных соискателей, работников и их родственников от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий.

1.4. Положение разработано в целях:

- обеспечения защиты прав и свобод субъектов персональных данных при обработке персональных данных в Учреждении;
- установления процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации о персональных данных, иных правовых актов Российской Федерации, внутренних документов Учреждения по вопросам обработки и защиты персональных данных;
- определения целей обработки персональных данных в информационных системах персональных данных (далее - ИСПДн) в установленной сфере деятельности, включая содержание обрабатываемых персональных данных, категории субъектов персональных данных, данные которых обрабатываются, сроки обработки (в том числе хранения) обрабатываемых персональных данных, а также порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований;
- установления ответственности работников Учреждения, имеющих доступ к персональным данным субъектов персональных данных в ИСПДн, за невыполнение требований норм, регулирующих обработку персональных данных, установленных законодательством Российской Федерации, настоящим Положением и иными локальными актами Учреждения.

1.5. В Положении используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно. Иные термины, применяемые в настоящих Правилах, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты персональных данных.

2. Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращений
ПДн	Персональные данные
Роскомнадзор	Уполномоченный орган по защите прав субъектов персональных данных
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

3. Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Безопасность информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	ГОСТ Р 50922-2006
Доступность информации (ресурсов информационной системы)	Состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно	Р 50.1.056-2005
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя	Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
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	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»

Термин	Определение	Источник
	данных	
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем	ГОСТ Р 50739-95
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право	Р 50.1.056-2005

4. Правовое основание для обработки персональных данных:

- Конституция Российской Федерации (ст.ст. 23, 24);
- Трудовой кодекс Российской Федерации (ст.ст. 65, 66, 86-90, 166);
- Гражданский кодекс Российской Федерации (гл.гл. 39, 40, 52);
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- - постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (при наличии

смешанной обработки ПДн или обработки ПДн без использования средств автоматизации);
- Постановление Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты» (п. 2);
- Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством» (ч.4 ст.13);
- Устав Учреждения;
- согласия субъектов персональных данных на обработку их персональных данных, а также договора, выгодоприобретателем или поручителем в которых являются субъекты персональных данных.;
- Федеральный закон от 02.10.2007 г. № 229-ФЗ «Об исполнительном производстве» (гл. 11);
- Семейный кодекс Российской Федерации (гл. 17);
- Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ (п. 2 ст. 9);
- Налоговый кодекс Российской Федерации (ст.ст.226, 230, 24);
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (ст.ст.6, 9, 11);
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации» (ст.11);
- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» (ст. 38);
- Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (ст.ст. 14, 17);
- Федеральный закон от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда» (ч. 2 ст. 4, ст.ст. 7, 8);
- Постановление Правительства РФ от 24.12.2021 № 2464 «О порядке обучения по охране труда и проверки знания требований охраны труда» (пп. 86, 87, 90, 92);
- Федеральный закон «О воинской обязанности и военной службе» от 28.03.1998 № 53-ФЗ (п. 7 ст. 8);
- Федеральный закон «Об обороне» от 31.05.1996 N 61-ФЗ (подп. 6 п. 1 ст. 8);
- Приказ Минобороны от 22.11.2021 № 700;
- Постановление Правительства РФ от 27.11.2006 N 719 «Об утверждении Положения о воинском учете»;
- Письмо ФНС России от 10 марта 2021 г. № БВ-4-7/3060@ (п. 15).

5. Количество субъектов ПДн, чьи ПДн обрабатываются в информационной системе персональных данных менее 100 тысяч.

6. Цели обработки персональных данных, их категории и перечень, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных:

1. Цель обработки: организация трудоустройства кандидатов на работу (соискателей)

Категории данных	Персональные данные	Специальные данные
Перечень данных	• фамилия, имя, отчество; • предыдущие фамилия, имя, отчество, если изменялись; • пол; • информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); • дата и место рождения; • изображение (фотография); • паспортные данные; • адрес регистрации по месту жительства; • адрес фактического проживания; • контактные данные; • страховой номер индивидуального лицевого счета (СНИЛС); • сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации; • семейное положение, наличие детей, родственные связи; • сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий; • данные о регистрации брака; • сведения о воинском учете; • сведения об инвалидности; • сведения о судимости, привлечении к уголовной ответственности; • информация о государственных наградах, иных наградах и знаков отличия; • сведения об ученой степени, ученом звании; • адрес электронной почты; • номер контактного телефона; • иные персональные данные, предоставляемые соискателями по их желанию	Сведения о состоянии здоровья
Категории субъектов	Кандидаты на работу (соискатели)	
Способы обработки	Автоматизированная обработка и без средств автоматизации	
Сроки обработки	В течение срока, необходимого для рассмотрения кандидатуры соискателя и заключения трудового договора	
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные, в том числе для анкеты (резюме) соискателя – 30 дней	
Порядок уничтожения	В соответствии с Порядком уничтожения и обезличивания персональных данных Учреждения в зависимости от типа носителя персональных	

<table>
<tr><td></td><td>данных</td><td></td></tr>
<tr><td colspan="3">2.Цель обработки: выполнения функций и полномочий работодателя в трудовых отношениях, в том числе обязанностей по охране труда.
В том числе:
–Осуществление хозяйственной деятельности, предусмотренной учредительными документами;
–соблюдение трудового законодательства и иных актов, содержащих нормы трудового права, включая учет труда и его оплаты, принятие управленческих и кадровых решений в отношении сотрудников, контроль над трудовой дисциплиной;
–участие в гражданском, арбитражном, уголовном, административном процессах, а также исполнение судебных актов;
–ведение бухгалтерского учета, осуществление расчета и выплаты сотрудникам причитающейся им заработной платы, компенсаций и премий, осуществление пенсионных и налоговых отчислений, а также расчет с подотчетными лицами;
–выпуск электронной-цифровой подписи, оформление доверенностей в рамках наделения сотрудников и иных лиц специальными полномочиями для выполнения возложенных на них трудовых функций и (или) представления интересов Учреждения;
–организация обучения, инструктажа, проверки знаний сотрудников и иных лиц по охране труда и технике безопасности, а также проведение специальной оценки условий труда, проведение оценки профессиональных рисков на рабочем месте;
–организация и (или) осуществление обучения, повышения квалификации и проверки знаний для своих сотрудников;
–организация ведения воинского учета работников - граждан Российской Федерации, создание необходимых условий для исполнения ими воинской обязанности; осуществление аттестации сотрудников посредством оценки их деловых и личностных качеств, а также результатов их труда;
– осуществление расследования и учета несчастных случаев, происшедших с сотрудниками и иными лицами при исполнении ими своих трудовых функций, а также в иных случаях, предусмотренных трудовым законодательством;
–публикация данных сотрудников на сайте Учреждения, внутренних справочниках;
–осуществление надлежащего учета, хранения и уничтожения по истечении сроков хранения категорий материальных носителей информации;
–исполнение обязательств появившихся при заключении договорных отношений; замещение вакантных должностей соискателями, наиболее полно соответствующими должностным требованиям.</td></tr>
<tr><td>Категории данных</td><td>Персональные данные</td><td>Специальные персональные данные</td><td>Биометрические персональные данные</td></tr>
<tr><td>Перечень данных</td><td>• фамилия, имя, отчество;
• предыдущие фамилия, имя, отчество, если изменялись;
• пол;
• информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
• дата и место рождения;
• изображение (фотография);
• паспортные данные;
• адрес регистрации по месту</td><td>Сведения о состоянии здоровья</td><td>Изображение на фото и видеозаписи, полученных с камер наблюдения</td></tr>
</table>

	жительства; • адрес фактического проживания; • контактные данные; • страховой номер индивидуального лицевого счета (СНИЛС); • сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации; • семейное положение, наличие детей, родственные связи; • сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий; • данные о регистрации брака; • сведения о воинском учете; • сведения об инвалидности; • сведения о судимости, привлечении к уголовной ответственности; • информация о государственных наградах, иных наградах и знаков отличия; • сведения об ученой степени, ученом звании; • адрес электронной почты; • номер контактного телефона; • иные персональные данные, предоставляемые работниками по их желанию		
Категории субъектов	Действующие и уволенные сотрудники (по ТК РФ), включая руководителя и лица, состоящие в родстве; Работники, не связанные трудовыми отношениями;		
Способы обработки	Автоматизированная обработка и без средств автоматизации, в том числе: • получение персональных данных в устной и письменной форме непосредственно от субъектов персональных данных; • внесения персональных данных в журналы, реестры и информационные системы и документы Учреждения		
Сроки обработки	В течение срока действия трудового договора		
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные, в том числе в составе личных дел – 50 лет		
Порядок	В соответствии с Порядком уничтожения и обезличивания персональных		

уничтожения	данных Учреждения в зависимости от типа носителя персональных данных
3.Цель обработки: реализация гражданско-правовых договоров, стороной, выгодоприобретателем или получателем которых является Учреждение, в том числе: –принятие мер должной осмотрительности при взаимодействии с действительными и потенциальными контрагентами (агентами, партнерами, подрядчиками, поставщиками), включающее в себя оценку соответствующих юридических, финансовых, репутационных и иных рисков; –связь с субъектами ПДн по вопросам, относящимся к предметам деятельности, а также взаимодействие с должностными/физическими лицами, представляющими юридические лица и индивидуальных предпринимателей, по вопросам сотрудничества с Учреждением; –осуществление взаимных расчетов с контрагентами (клиентами, агентами, партнерами, подрядчиками, поставщиками); –поставка товаров, выполнение работ и оказание услуг, в пользу Учреждения со стороны контрагентов (поставщиков), а также осуществление процедур закупок у указанных контрагентов и ведение деловых переговоров с указанными контрагентами; –предоставление доступа к сервисам и информации, размещенной на сайте Учреждения	
Категории данных	Персональные данные
Перечень данных	• фамилия, имя, отчество; • паспортные данные; • адрес регистрации и (или) фактического проживания; • контактные данные; • индивидуальный номер налогоплательщика; • страховой номер индивидуального лицевого счета (СНИЛС); • номер расчетного счета; • номер банковской карты; • иные персональные данные, предоставляемые физическими лицами, необходимые для заключения и исполнения договоров
Категории субъектов	Контрагенты, партнеры, стороны договора
Сроки обработки	• В течение срока, необходимого для исполнения заключенного договора
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные
Порядок уничтожения	В соответствии с Порядком уничтожения и обезличивания персональных данных Учреждения в зависимости от типа носителя персональных данных

7. Сбор, обработка и хранение персональных данных

7.1. Сбор персональных данных соискателей осуществляет должностное лицо Учреждения, которому поручен подбор кадров, в том числе из общедоступной информации о соискателях в интернете.

7.2. Сбор персональных данных работников осуществляет работник, назначенный руководителем Учреждениям, у самих работников. Если персональные

данные работника можно получить только у третьих лиц, Учреждение уведомляет об этом работника и берет у него письменное согласие на получение данных.

7.3. Сбор персональных данных родственников работника осуществляется со слов работника и из документов, которые предоставил работник.

7.4. Обработка персональных данных соискателей ведется исключительно в целях определения возможности их трудоустройства.

7.5. Обработка персональных данных работников ведется исключительно в целях обеспечения соблюдения законодательства РФ, содействия работникам в трудоустройстве, получении образования, продвижении по службе, обеспечения их личной безопасности и сохранности имущества, контроля количества и качества выполняемой ими работы.

7.6. Обработка персональных данных родственников работников ведется исключительно в целях обеспечения соблюдения законодательства РФ, реализации прав работников, предусмотренных трудовым законодательством и иными актами, содержащими нормы трудового права.

7.7. Сбор и обработка персональных данных, которые относятся к специальной категории (сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни) возможны только с согласия субъекта персональных данных либо в случаях, установленных законодательством о персональных данных.

7.8. Сбор и обработка персональных данных родственников работников, которые относятся к специальной категории (сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни), не допускаются.

7.9. Сбор и обработка персональных данных соискателей, работников и их родственников о членстве в общественных объединениях или профсоюзной деятельности не допускаются, за исключением случаев, предусмотренных федеральными законами.

7.10. Личные дела, трудовые и медицинские книжки работников хранятся в бумажном виде в папках в кабинете, определенном руководителем Учреждения, в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа.

7.11. Документы, содержащие личную информацию о работнике, кроме указанных в пункте 3.10 Положения, хранятся в бумажном виде в отделе кадров и в электронном виде в информационных системах.

7.12. Документы соискателя, который не был трудоустроен, уничтожаются в течение 30 дней с момента принятия решения об отказе в трудоустройстве.

7.13. Документы, содержащие персональные данные работников и родственников работников, подлежат хранению и уничтожению в сроки и в порядке, предусмотренные номенклатурой дел и архивным законодательством РФ.

7.14. Работники вправе требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями требований Трудового кодекса или иного федерального закона.

7.15. Персональные данные оценочного характера работник вправе дополнить заявлением, выражающим его собственную точку зрения.

8. Доступ к персональным данным

8.1. Доступ к персональным данным соискателя, работников и их родственников имеет руководитель Учреждения в полном объеме.

8.2. Перечень работников, допущенных к обработке персональных данных соискателей, работников и их родственников, утверждается приказом руководителя Учреждения.

9. Передача персональных данных.

9.1. Работники Учреждения, имеющие доступ к персональным данным соискателей, работников и их родственников, при передаче этих данных должны соблюдать следующие требования:

9.1.1. Не передавать и не распространять персональные данные без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо:

- для предупреждения угрозы жизни и здоровью субъекта персональных данных, если получить такое согласие невозможно;
- для статистических или исследовательских целей (при обезличивании);
- в случаях, напрямую предусмотренных федеральными законами.

9.1.2. Передавать без согласия субъекта персональных данных информацию в государственные и негосударственные функциональные структуры, в том числе в налоговые инспекции, фонд медицинского страхования, социальный фонд, правоохранительные органы, страховые агентства, военкоматы, медицинские организации, контрольно-надзорные органы при наличии оснований, предусмотренных в федеральных законах, или мотивированного запроса от данных структур, если это допускается законодательством РФ.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

9.1.3. Передавать персональные данные представителям работников и соискателей в порядке, установленном Трудовым кодексом, ограничивая эту информацию только теми персональными данными, которые необходимы для выполнения функций представителя, подтвержденных документально.

10. Меры обеспечения безопасности персональных данных

10.1. К основным мерам обеспечения безопасности персональных данных в Учреждении относятся:

10.1.1. Назначение ответственного за организацию обработки персональных данных, в обязанности которого входит в том числе организация обработки персональных данных, обучение и инструктаж работников, внутренний контроль за соблюдением в Учреждении требований законодательства к защите персональных данных.

10.1.2. Издание политики обработки персональных данных и локальных актов по вопросам обработки персональных данных.

10.1.3. Ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями к защите персональных данных, политикой обработки персональных данных и локальными актами Учреждения по вопросам обработки персональных данных.

10.1.4. Определение угроз безопасности персональным данным при их обработке с использованием средств автоматизации и разработка мер по защите таких персональных данных.

10.1.5. Учет материальных носителей персональных данных.

10.1.6. Проведение мероприятий при обнаружении несанкционированного доступа к персональным данным, обрабатываемым с использованием средств автоматизации, в том числе восстановление персональных данных, которые были модифицированы или уничтожены вследствие несанкционированного доступа к ним.

10.1.7. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства о персональных данных, оценка соотношения указанного вреда и принимаемых мер.

10.1.8. Внутренний контроль соответствия обработки персональных данных требованиям законодательства.

10.1.9. Публикация политики обработки персональных данных и локальных актов по вопросам обработки персональных данных на официальном сайте Учреждения.

10.1.10.Организация уведомления Роскомнадзора в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, в соответствии с законодательством о персональных данных.

10.1.11.Обеспечение взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных, в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

11. Ответственность.

11.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных соискателей на вакантные должности, работников, в том числе бывших, и их родственников, привлекаются к дисциплинарной и материальной, гражданско-правовой, административной и уголовной ответственности в случаях, установленных законодательством РФ.

11.2. Моральный вред, причиненный соискателям на вакантные должности, работникам, в том числе бывшим, и их родственникам вследствие нарушения их прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, подлежит возмещению в порядке и на условиях, предусмотренных законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда.

12. Срок (условия прекращения) обработки персональных данных, в том числе их хранения:

- ликвидация, реорганизация, прекращение деятельности Учреждения;
- достижение целей обработки персональных данных и максимальных сроков хранения;
- утрата необходимости в достижении целей обработки;

- предоставление субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными для заявленной цели обработки;
- невозможность обеспечения правомерности обработки персональных данных;
- отзыв субъектом персональных данных согласия на обработку ПДн.

Приложение № 3

УТВЕРЖДЕНЫ
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Правила
обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Правила) разработаны в целях:

- обеспечения защиты прав и свобод субъектов персональных данных при обработке персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение);
- установления процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации о персональных данных, иных правовых актов Российской Федерации, внутренних документов Учреждения по вопросам обработки и защиты персональных данных;
- определения целей обработки персональных данных в информационных системах персональных данных (далее - ИСПДн) в установленной сфере деятельности субъектов персональных данных, данные которых обрабатываются, сроки обработки (в том числе хранения) обрабатываемых персональных данных, а также порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований;
- установления ответственности работников Учреждения, имеющих доступ к персональным данным субъектов персональных данных в ИСПДн, за невыполнение требований норм, регулирующих обработку персональных данных, установленных законодательством Российской Федерации, настоящими Правилами и иными локальными актами Учреждения.

1.2. В настоящих Правилах используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно. Иные термины, применяемые в настоящих Правилах, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты персональных данных.

Таблица 1 – Перечень сокращений

Сокращение	**Расшифровка сокращений**
ПДн	Персональные данные
Роскомнадзор	Уполномоченный орган по защите прав субъектов персональных данных
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Таблица 2 – Перечень терминов и определений

Термин	**Определение**	**Источник**
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный зако Российской Федерации о 27.06.2006 № 152-ФЗ «(персональных данных»
Безопасность информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	ГОСТ Р 50922-2006
Доступность информации (ресурсов информационной системы)	Состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно	Р 50.1.056-2005
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон о 27.06.2006 № 152-ФЗ «(персональных данных»
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя	Федеральный закон о 27.06.2006 № 149-ФЗ «О информации, информационных технологиях и о защит информации»
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	Федеральный закон о 27.06.2006 № 152-ФЗ «(персональных данных»
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российско Федерации от 15.09.2008 N 687 «Об утверждени Положения о особенностях обработк персональных данных осуществляемой бе использования средст автоматизации»

Термин	Определение	Источник
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон о 27.06.2006 № 152-ФЗ «(персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный зако Российской Федерации о 27.06.2006 № 152-ФЗ «(персональных данных»
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем	ГОСТ Р 50739-95
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право	Р 50.1.056-2005

1.3. Настоящие Правила разработаны на основании следующих нормативных правовых актов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (при наличии смешанной обработки ПДн или обработки ПДн без использования средств автоматизации).

1.4. Настоящие Правила устанавливают и определяют в Учреждении:

- процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки и защиты ПДн;
- цели обработки ПДн;
- содержание обрабатываемых ПДн;
- категории субъектов, ПДн которых обрабатываются;
- сроки обработки и хранения обрабатываемых ПДн;
- порядок уничтожения обработанных ПДн при достижении целей обработки или при наступлении иных законных оснований.

1.5. Правила являются обязательными для исполнения всеми пользователями ИСПДн, имеющими доступ к ПДн.

Пользователи ИСПДн должны быть ознакомлены с настоящими Правилами до начала работы в ИСПДн под подпись.

Обязанность по организации ознакомления пользователей с настоящими Правилами возлагается на ответственного за организацию обработки ПДн.

1.6. Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами.

2. Требования к обработке и защите ПДн

2.1. Учреждение при обработке ПДн руководствуется принципами и условиями, определенными нормами главы 2 Федерального закона № 152-ФЗ.

2.2. Права субъектов ПДн определены в главе 3 Федерального закона № 152-ФЗ.

2.3. При определении обязанностей Учреждением при сборе ПДн и при обращении субъектов ПДн в Учреждение руководствуется главой 4 Федерального закона № 152-ФЗ.

2.4. Учреждением принимаются меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, в том числе:

- распорядительным актом Учреждения назначается ответственный за организацию обработки ПДн в Учреждении и утверждается Инструкция ответственного за организацию обработки персональных данных в Учреждении, в которой определены его права и обязанности;
- составляется перечень ПДн, обрабатываемых в ИСПДн, который утверждается распорядительным актом Учреждения;
- издаются документы, определяющие политику Учреждения в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, определяющих для каждой цели обработки ПДн объем, категории и перечень обрабатываемых ПДн, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;
- обеспечивается размещение на официальном сайте Учреждения Политики в отношении обработки персональных данных в Учреждении;
- применяются правовые, организационные и технические меры по обеспечению безопасности ПДн в соответствии со статьей 19 Федерального закона № 152-ФЗ «О персональных данных»;
- осуществляется внутренний контроль соответствия обработки ПДн Федеральному закону № 152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актам, локальным актам Учреждения согласно Правилам внутреннего контроля обработки персональных данных на соответствие требованиям к их защите, утвержденным в Учреждении;
- обеспечивается ознакомление пользователей ИСПДн, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской

Федерации, локальными актами оператора в сфере обработки ПДн, в том числе требованиями к защите ПДн и настоящими Правилами;

- запрещается обработка ПДн в ИСПДн, а равно и обработка ПДн без использования средств автоматизации (при наличии смешанной обработки ПДн), работниками, не допущенными к обработке ПДн согласно распорядительному акту Учреждения о предоставлении пользователям доступа к информационным ресурсам информационных систем персональных данных в Учреждении.

2.5. Обработка ПДн осуществляется после получения согласия субъекта ПДн (за исключением случаев, предусмотренных частью 1 статьи 6 Федерального закона № 152-ФЗ «О персональных данных»), при условии выполнения требований к защите ПДн.

Согласие на обработку субъект ПДн предоставляет письменно по форме согласно *Приложению № 1 к настоящим Правилам*.

2.6. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, предоставляется письменно по форме согласно *Приложения № 2 к настоящим Правилам*. При необходимости оператор обязан обеспечить субъекту ПДн возможность определить перечень ПДн по каждой категории ПДн, указанной в согласии на обработку ПДн, разрешенных субъектом ПДн для распространения.

2.7. При необходимости привлечения к обработке ПДн третьих лиц оператор ПДн может передать для обработки персональные данные субъекта ПДн третьему лицу только с согласия субъекта ПДн. В этом случае согласие на передачу субъект ПДн предоставляет письменно по форме *согласно Приложения № 3 к настоящим Правилам*.

2.8. В случае, когда в информационной системе персональных данных обрабатываются ПДн несовершеннолетних и в соответствии с законодательством Российской Федерации требуется согласие от законного представителя оформляется согласие законного представителя на обработку ПДн несовершеннолетнего по форме согласно *Приложения № 4 к настоящим Правилам*.

2.9. Безопасность ПДн, при их обработке в ИСПДн, обеспечивает Учреждение.

2.10. При обработке ПДн соблюдаются следующие требования:

- к работе с ПДн допускаются только пользователи ИСПДн на основании соответствующего распорядительного акта Учреждения, и подписавшие обязательство о неразглашении персональных данных по форме согласно *Приложения № 5 к настоящим правилам*;
- в целях обеспечения сохранности документов, содержащих ПДн, все операции по оформлению, формированию, ведению и хранению данной информации выполняются пользователями – работниками Учреждения, осуществляющими данную деятельность в связи с исполнением трудовых (служебных) обязанностей, изложенных в их должностных инструкциях;
- на период обработки ПДн в помещении могут находиться только лица, допущенные в установленном порядке к обработке ПДн.

2.11. Особенности обработки ПДн:

1) машинные носители ПДн подлежат обязательной регистрации и учету;

2) обработка ПДн осуществляется при условии выполнения требований к защите ПДн, утвержденных:

- постановлением Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- локальными актами Учреждения, устанавливающими принятие организационных и технических мер для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

2.12. Работники, осуществляющие обработку персональных данных без использования средств автоматизации, проинформированы в соответствии с формой *согласно Приложению № 6 к настоящим Правилам* о факте обработки ими персональных данных, обработка которых осуществляется в Учреждении без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами Российской Федерации, а также локальными правовыми актами Учреждения.

В целом порядок обработки персональных данных, осуществляемой без использования средств автоматизации, определяется Политикой в отношении обработки персональных данных в Учреждении.

3. Цели обработки ПДн:

3.1. Целями обработки ПДн, содержание обрабатываемых ПДн, категории ПДн в Учреждении определяются в Положении об обработке персональных данных в Учреждении.

4. Сроки обработки и хранения обрабатываемых ПДн.

4.1. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

4.2. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3. Основания для прекращения обработки ПДн и сроки их уничтожения определены в частях 3, 4, 5, 5.1 статьи 21 Федерального закона № 152-ФЗ.

4.4. Основанием (условием) прекращения обработки ПДн также является ликвидация либо реорганизация Учреждения.

4.5. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в частях 3, 4, 5, 5.1 статьи 21 Федерального закона № 152-ФЗ, Учреждение осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения). Обеспечивает уничтожение ПДн в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

5. Порядок уничтожения ПДн

5.1. Уничтожение персональных данных осуществляется в соответствии с Положением о комиссии Учреждения по уничтожению персональных данных согласно *Приложению № 7 к настоящим Правилам*.

5.2. Порядок уничтожения машинного носителя персональных данных определяется Инструкцией по защите машинных носителей персональных данных в Учреждении согласно *Приложению № 8 к настоящим Правилам*.

6. Ответственность за нарушения при обработке ПДн

6.1. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, установленных настоящими Правилами, в соответствии с действующим законодательством Российской Федерации.

7. Заключительные положения

7.1. Работники, определенные распорядительным актом Учреждения, как пользователи ИСПДн, участвующие в обработке и защите ПДн, должны быть ознакомлены с настоящими Правилами.

7.2. Обязанность по организации работы по ознакомлению под подпись работников Учреждения с положениями нормативных правовых актов Российской Федерации в сфере обработки и защиты ПДн, локальных актов Учреждения по вопросам обработки ПДн, требованиями к защите ПДн, возлагается на ответственного за организацию обработки ПДн в Учреждении.

Приложение № 1
к Правила обработки персональных данных
в Муниципальном учреждении «Всеволожский
районный методический центр»

Согласие субъекта персональных данных на обработку персональных данных

Я, _____
(фамилия, имя, отчество)
документ, удостоверяющий личность _____ серия _____ № _____,
(вид документа)
выдан _____
(кем и когда)
зарегистрированный (ая) по адресу:

_____

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных) даю свое согласие МУ «ВРМЦ» (ОГРН: 1084703005749, ИНН: 4703107467), зарегистрированному по адресу: 188640, Ленинградская обл., Всеволожский р-н, г. Всеволожск, Колтушское шоссе, д. 99 (далее - Оператор) на обработку своих персональных данных.

1. Цель обработки персональных данных: _____
2. Перечень персональных данных, передаваемых на обработку: _____
3. Перечень действий с персональными данными, осуществляемых Оператором: _____
(указывается общее описание используемых Оператором способов обработки персональных данных)
4. Настоящее согласие вступает в силу со дня его подписания и действует до истечения определяемых в соответствии с законодательством Российской Федерации сроков хранения персональных данных.
5. Мне разъяснены мои права и обязанности, в части обработки персональных данных, в том числе, моя обязанность проинформировать оператора в случае изменения персональных данных.

«____» _____ 20___ г. _____ _____
(подпись) ФИО

Приложение № 2

к Правила обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

Согласие субъекта персональных данных на обработку персональных данных, разрешенных субъектом ПДн для распространения

Я, _____
(Ф.И.О. работника полностью)

руководствуясь ст. 10.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», заявляю о согласии на распространение Муниципальным учреждением «Всеволожский районный методический центр» (далее – МУ «ВРМЦ») моих персональных данных с целью размещения информации обо мне в информационно-коммуникационной сети Интернет и на официальном сайте МУ «ВРМЦ»
в следующем порядке:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да / нет)	Неограниченному кругу лиц (да / нет)	Условия и запреты	Дополнительные условия
общие персональные данные	фамилия				
	имя				
	отчество				
	образование				
	профессия				
	Электронная почта				
	Телефон рабочий				
	Информация о награждениях				
	Стаж работы				
фотография	цветное цифровое фотографическое изображение лица				

Сведения об информационных ресурсах МУ «ВРМЦ» (оператора), посредством которых будет осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
https://rmc.vsevobr.ru/	Предоставление сведений неограниченному кругу лиц
https://vk.com/id551939225	Предоставление сведений неограниченному кругу лиц

Настоящее согласие дано мной добровольно и действует до отзыва в установленном законом порядке.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования Оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

«____» _____ 20___ г. _____ _____
(подпись) ФИО

Приложение № 3
к Правила обработки персональных данных
в Муниципальном учреждении «Всеволожский
районный методический центр»

Согласие субъекта персональных данных на передачу персональных данных

Я, _____
(фамилия, имя, отчество)
документ, удостоверяющий личность _____ серия_____ № _____,
(вид документа)
выдан_____
(кем и когда)
зарегистрированный (ая) по адресу: _____

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных) даю свое согласие МУ «ВРМЦ» (ОГРН: 1084703005749, ИНН: 4703107467), зарегистрированному по адресу: 188640, Ленинградская обл., Всеволожский р-н, г. Всеволожск, Колтушское шоссе, д. 99 (далее - Оператор) на передачу своих персональных данных в _____
(указывается наименование организации третьего лица, реквизиты организации третьего лица)

1. Цель передачи персональных данных: _____
2. Перечень передаваемых персональных данных: _____
(указывается перечень передаваемых персональных данных)
3. Перечень действий с персональными данными, осуществляемых Оператором_____
(указывается общее описание используемых Оператором способов обработки персональных данных)
4. Настоящее согласие вступает в силу со дня его подписания и действует до истечения определяемых в соответствии с законодательством Российской Федерации сроков хранения персональных данных.
5. Ответственность за обеспечение сохранности и конфиденциальности передаваемых персональных данных и за нарушения _____
(наименование организации третьего лица)
при обработке переданных персональных данных несет оператор персональных данных МУ «ВРМЦ».

«____» _____ 20___ г. _____
(подпись)

Приложение № 4

к Правила обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

Согласие законного представителя на обработку персональных данных несовершеннолетнего

Я, _____
(фамилия, имя, отчество)
документ, удостоверяющий личность _____ серия_____ № _____,
(вид документа)
выдан_____
(кем и когда)
зарегистрированный (ая) по адресу: _____
являюсь законным представителем субъекта персональных данных: _____
Свидетельство о рождении серия _____№_____ выдано (кем и когда): _____
на основании статьи 64 Семейного кодекса Российской Федерации (или указывается иное правовое основание» в соответствии со в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных) даю свое согласие МУ «ВРМЦ» (ОГРН: 1084703005749, ИНН: 4703107467), зарегистрированному по адресу: 188640, Ленинградская обл., Всеволожский р-н, г. Всеволожск, Колтушское шоссе, д. 99 (далее - Оператор) на обработку персональных данных.

1. Цель передачи персональных данных: _____
2. Перечень передаваемых персональных данных: _____
(указывается перечень передаваемых персональных данных)
3. Перечень действий с персональными данными, осуществляемых Оператором_____
(указывается общее описание используемых Оператором способов обработки персональных данных)
4. Настоящее согласие вступает в силу со дня его подписания и действует до истечения определяемых в соответствии с законодательством Российской Федерации сроков хранения персональных данных.
5. Согласие может быть досрочно отозвано путем подачи письменного заявления в адрес Оператора.
6. Я предупрежден(а), что в случае отзыва согласия на обработку персональных данных, Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пп. 2-11 ч. 1 ст. 6 и ч. 2 ст. 10 Федерального закона «О персональных данных».

«____» _____ 20___ г. _____
(подпись)

Приложение № 5
к Правила обработки персональных данных
в Муниципальном учреждении «Всеволожский
районный методический центр»

Обязательство о неразглашении персональных данных

Я, _____

паспорт серии _____ номер _____, выданный «_____» _____ _____ года в период трудовых (служебных) отношений с МУ «ВРМЦ» и в течение _____ лет после их прекращения в соответствии с Политикой в отношении обработки персональных данных и требованиями к защите информации в МУ «ВРМЦ» обязуюсь:

1. не разглашать и не передавать третьим лицам сведения, содержащие персональные данные, которые мне будут доверены или станут известны по работе, кроме случаев, предусмотренных законодательством Российской Федерации и с разрешения ответственного за организацию обработки персональных данных в организации;
2. выполнять требования приказов, положений и инструкций по обработке персональных данных в части меня касающейся;
3. в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, а также в случае утери носителей информации, содержащих такие сведения, немедленно сообщить об этом лицу, ответственному за организацию обработки персональных данных;
4. не производить преднамеренных действий, нарушающих достоверность, целостность или конфиденциальность персональных данных, хранимых и обрабатываемых в МУ «ВРМЦ».

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности персональных данных при автоматизированной обработке информации и осуществляемой без средств автоматизации.

Мне известно, что нарушение этого обязательства может повлечь ответственность, предусмотренную трудовым, административным и уголовным законодательством Российской Федерации.

«____» _____ 20___ г. _____

(подпись)

Приложение № 6

к Правила обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

Согласие на обработку персональных данных

Я, _____,

в соответствии со статьей 9 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- исчисления и уплаты предусмотренных законодательством Российской Федерации налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд Российской Федерации, сведений подоходного налога в ФНС России, сведений в Фонд Социального Страхования Российской Федерации;
- предоставления налоговых вычетов;
- обеспечения моей безопасности.

своей волей и в своих интересах выражаю согласие на осуществление оператором (работодателем) – *Муниципальному учреждению «Всеволожский районный методический центр»* на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление, доступ, обезличивание, блокирование, удаление, уничтожение персональных данных.

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный);
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;
- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;
- номер СНИЛС;
- номер ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в Муниципальном учреждении «Всеволожский районный методический центр»;

— фотография;
— информацию о наличии либо отсутствии судимости.

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Работодателю (оператору) заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать в двухнедельный срок об изменении местожительства, контактных телефонов, паспортных, документных и иных персональных данных. Об ответственности за достоверность представленных персональных сведений предупрежден(а).

«____» _____ 20___ г. _____

(подпись)

Приложение № 7
к Правилам обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

Положение о комиссии
Муниципального учреждения «Всеволожский районный методический центр»
по уничтожению персональных данных

1. Общие положения

1.1. Настоящее Положение о комиссии Муниципального учреждения «Всеволожский районный методический центр» по уничтожению персональных данных (далее - Положение) разработано в целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», которым определяется порядок уничтожения персональных данных в Муниципального учреждения «Всеволожский районный методический центр» (далее – Учреждение) в случаях, установленных действующим законодательством Российской Федерации.

1.2. В настоящем Положении используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Иные термины, применяемые в настоящем Правилах, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты персональных данных.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращений
Комиссия	Комиссия Учреждения по уничтожению персональных данных
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Администратор информационной безопасности	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе	постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»

Термин	Определение	Источник
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	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

1.3. Настоящее Положение разработано на основании следующих нормативных правовых актов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

1.4. Комиссия состоит из председателя Комиссии и не менее двух членов Комиссии.

1.5. Председатель и члены Комиссии назначаются распорядительным актом Учреждения.

1.6. Председателем Комиссии определяется лицо, назначенное ответственным за организацию обработки персональных данных в Учреждении.

1.7. Членами Комиссии назначаются руководители структурных подразделений Учреждения и/или заместители руководителей, а также работник, ответственный за обеспечение безопасности персональных данных (далее - администратор безопасности) и работник, ответственный за ведение бухгалтерского учета Учреждения.

1.8. Комиссия в своей работе руководствуется Положением о Комиссии.

1.9. Периодичность, дата, время и место заседания Комиссии определяется председателем Комиссии.

1.10. Предложения по уничтожению (стиранию) персональных данных на машинных[1] носителях персональных данных и (или) бумажных носителях персональных данных, а также в информационных системах персональных данных подготавливаются членами Комиссии для их последующего рассмотрения Комиссией.

1.11. В случае принятия решения об уничтожении персональных данных составляется акт об уничтожении персональных данных по форме согласно *Приложению к настоящему Положению*.

1.12. В случае, если обработка персональных данных осуществляется с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных, являются акт об уничтожении персональных данных (далее - Акт), соответствующий требованиям, содержащимся в пунктах 1.13 и 1.14 настоящего Положения, и выгрузка из журнала регистрации событий в соответствующей информационной системе персональных данных (далее – выгрузка из журнала).

1.13. Акт должен содержать:

а) наименование должности, фамилию, инициалы руководителя Учреждения, утвердившего Акт и адрес Учреждения;

б) фамилию, имя, отчество (при наличии) субъекта (субъектов персональных данных) или иную, информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

в) фамилии, имена, отчества (при наличии) председателя и членов Комиссии, уничтоживших персональные данные субъекта персональных данных, а также их подписи;

г) перечень уничтоженных категорий персональных данных субъекта (субъектов) персональных данных;

д) наименование уничтоженного материального (материальных) носителей, содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

---

[1] Под машинными носителями персональных данных понимаются съемные и несъемные носители персональных данных, используемые для передачи и хранения персональных данных в электронном виде.

е) наименование информационной (информационных) системы (систем) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

ж) способ уничтожения персональных данных;

з) причину уничтожения персональных данных;

и) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

1.14. Акт в электронной форме, подписанный в соответствии с законодательством Российской Федерации, признается электронным документом, равнозначным Акту на бумажном носителе, пописанному собственноручной подписью лиц, указанных в подпунктах «а» и «в» пункта 1.13 настоящего Положения.

1.15. Выгрузка из журнала должна содержать:

а) фамилию, имя, отчества (при наличии) субъекта (субъектов) персональных данных или иную, информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

б) перечень уничтоженных категорий персональных данных субъекта (субъектов) персональных данных;

в) наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

г) причину уничтожения персональных данных;

д) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

1.16. В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные пунктом 1.15 настоящего Положения, недостающие сведения вносятся в Акт.

1.17. В случае, если обработка персональных данных осуществляется в Учреждении одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются Акт, соответствующий требованиям, установленным пунктами 1.13 и 1.14 настоящего Положения, и выгрузка из журнала, соответствующая требованиям, установленным пунктом 1.15 настоящего Положения.

1.18. Запись об уничтожении машинного носителя персональных данных в Журнал учета машинных носителей персональных данных в Учреждении вносит администратор безопасности с указанием соответствующего номера и даты утвержденного Акта руководителем Учреждения.

1.19. Работник, ответственный за ведение бухгалтерского учета в Учреждении, организует подготовку документов на списание машинного носителя персональных данных, не подлежащего дальнейшей эксплуатации.

2. Порядок уничтожения (стирания) персональных данных.

2.1. Уничтожение (стирание) персональных данных осуществляется в случаях:

- достижения целей обработки персональных данных;
- отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- выявления неправомерных действий с персональными данными, а также в иных случаях, предусмотренных действующим законодательством Российской Федерации.

2.2. Комиссия при решении вопроса об уничтожении персональных данных принимает во внимание, что в случае достижения цели обработки персональных данных Учреждение прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных.

2.3. Также Комиссией учитывается, что в случае, если субъект персональных данных отозвал свое согласие на обработку персональных данных Учреждение прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных.

2.4. Комиссия обязана также учитывать, что в случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением, или лицом, действующим по поручению Учреждения, и невозможности обеспечить правомерность обработки персональных данных, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение.

Об уничтожении персональных данных Учреждение уведомляет субъект персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

2.5. Комиссия обязана обеспечивать уничтожение (стирание) персональных данных, а также контроль за её уничтожением (стиранием) при передаче машинных носителей персональных данных между пользователями, в сторонние организации для ремонта или утилизации.

Уничтожение персональных данных на машинных носителях персональных данных осуществляется с оформлением Акта.

2.6. Комиссия осуществляет отбор материальных носителей персональных данных, подлежащих уничтожению.

2.7. По окончании отбора материальных носителей персональных данных, подлежащих уничтожению, и их фактического уничтожения (стирания) всем

составом Комиссии подписывается Акт по форме *в соответствии с Приложением* и передается на утверждение руководителю Учреждения.

2.8. В случае, если Комиссией принято решение об уничтожении персональных данных субъекта (субъектов) персональных данных в информационной системе персональных данных порядок уничтожения персональных определяется пунктом 1.12 настоящего Положения.

2.9. В Акте исправления не допускаются.

2.10. Уничтожение персональных данных на машинных носителях персональных данных, если это допускается машинным носителем персональных данных, может производиться способом, исключающим дальнейшую обработку персональных данных с сохранением возможности обработки иных данных, зафиксированных на машинном носителе.

2.11. Правила уничтожения (стирания) персональных данных:

- способ уничтожения персональных данных определяется Комиссией в зависимости от типа носителя персональных данных и возможностей Учреждения;
- стирание персональных данных на машинном носителе осуществляется по технологии, предусмотренной для данного типа носителя, с применением функций средств защиты информации (допускается задействовать механизмы затирания, встроенные в сертифицированные средства защиты информации);
- уничтожение материальных носителей персональных данных производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления персональных данных (перед уничтожением, если носитель исправен, должно быть произведено стирание персональных данных, содержащихся на носителе). Непосредственные действия по уничтожению конкретного типа носителя персональных данных должны быть достаточны для исключения возможности восстановления персональных данных;
- бумажные и прочие сгораемые материальные носители персональных данных уничтожают путем шредирования либо термической обработки.

2.12. Акт и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

Приложение
к Положению о комиссии Муниципального учреждения «Всеволожский районный методический центр» по уничтожению персональных данных

УТВЕРЖДАЮ
Наименование учреждения
Директор
ФИО

_____
(подпись, печать)

«___» _____ 20__ г.

Акт
об уничтожении персональных данных

Комиссия в составе:

Председатель комиссии:
Члены комиссии:

составила настоящий акт о том, что перечисленные в нем персональные данные уничтожены по месту нахождения Учреждения, расположенного по адресу: _____, по причине _____ «_____» _____ 20___ года .

№ п/п	Вид материального носителя	Номер материального носителя	Количество листов на уничтоженном	Серийный (заводской) номер	Наименование информационной системы	Фамилия, имя, отчество субъекта (субъектов)	Перечень уничтоженных категорий	Способ уничтожения персональных

	персональных данных (наименование машинного носителя персональных данных)[2]	персональных данных[3]	бумажном носителе персональных данных[4]	машинного носителя персональных данных	персональных данных[5]	персональных данных или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	персональных данных субъекта (субъектов) персональных данных	данных[6]

Персональные данные перед уничтожением сверены с записями в настоящем акте.

Председатель: _____ /_____/

Члены комиссии: _____ /_____/

_____ /_____/

---

[2] В указанной графе указывается вид материального носителя персональных данных – бумажный либо машинный (в случае, если уничтожены персональные данные на машинном носителе персональных данных, то его наименование)

[3] В указанной графе указывается номер бумажного носителя персональных данных согласно номенклатуре дел, либо учетный номер машинного носителя персональных данных согласно Журналу учета машинных носителей персональных данных в организации.

[4] Указывается количество листов уничтоженного бумажного носителя персональных данных (данная графа заполняется только в отношении уничтоженных бумажных носителей персональных данных)

[5] Данная графа заполняется в случае, если персональные данные уничтожаются в информационной системе персональных данных

[6] В указанной графе указывается способ уничтожения материального носителя персональных данных либо непосредственно персональных данных.

Приложение № 8
к Правилам обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

ИНСТРУКЦИЯ
по защите машинных носителей персональных данных
в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения.

1.1. Настоящая Инструкция по защите машинных носителей персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее - Инструкция) определяет порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей персональных данных, используемых в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение).

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФАПСИ	Федеральное агентство правительственной связи и информации при Президенте Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ФСБ России	Федеральная служба безопасности Российской Федерации
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
СВТ	Средства вычислительной техники
СКЗИ	Средство криптографической защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в ин формационной системе персональных данных	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Инцидент информационной	Одно или несколько нежелательных или не	ГОСТ Р ИСО/МЭК

Термин	Определение	Источник
безопасности	ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности	27000
Машинный носитель данных	Сменный носитель данных, предназначенный для записи и считывания данных, представленных в стандартных кодах	ГОСТ 25868-91
Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде.	
Машинный носитель персональных данных	Машинный носитель информации, на которых хранятся и (или) обрабатываются персональные данные	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
СКЗИ	Шифровальные (криптографические) средства защиты информации конфиденциального характера. К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСБ России 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 требованиям к защите персональных данных для каждого из уровней защищенности»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;

1.4. Работники, допущенные к обработке персональных данных в Учреждении в связи с необходимостью выполнения ими трудовых (служебных) обязанностей, (далее – работники) должны быть ознакомлены с настоящей Инструкцией до начала обработки персональных данных под подпись.

Обязанность по организации ознакомления работника с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Организация учета машинных носителей персональных данных.

2.1. Все используемые в Учреждении машинные носители персональных данных подлежат регистрации и учету, а именно:

- несъёмные машинные носители (жесткие диски, находящиеся в системных блоках серверов, в том числе во внешних RAID-массивах серверов, и системных блоках АРМ ИСПДн);
- съёмные машинные носители (флеш-память, SSd-диски, оптические носители персональных данных и пр. технические средства, предназначенные для запоминания информации, и оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) либо считывания с них информации в память АРМ (или сервера)).

2.2. Применение в Учреждении незарегистрированных машинных носителей персональных данных запрещается.

2.3. Приобретенные машинные носители информации перед использованием передаются администратору безопасности для регистрации.

2.4. Ответственным за регистрацию, хранение, выдачу машинных носителей персональных данных, ведение учетной документации и контроль уничтожения машинных носителей персональных данных в установленном порядке является администратор безопасности.

2.5. Ответственность по организации процедуры уничтожения машинных носителей персональных данных возлагается на ответственного за организацию обработки ПДн.

2.6. При смене администратора безопасности составляется акт приема-сдачи учетной документации и машинных носителей персональных данных.

3. Порядок учета машинных носителей персональных данных.

3.1. Основной учет машинных носителей персональных данных производится по Журналу учета машинных носителей персональных данных в Учреждении согласно *Приложению №1 к настоящей Инструкции.*

Ведение и надежное хранение Журнала учета машинных носителей персональных данных в Учреждении осуществляет администратор безопасности.

Срок хранения завершенного Журнала учета машинных носителей персональных данных в Учреждении определяется утвержденной номенклатурой Учреждения.

Уничтожение Журнала учета машинных носителей персональных данных в Учреждении по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Учреждении.

3.2. Учет осуществляется с использованием регистрационных (заводских) номеров.

3.3. Учетный номер каждого зарегистрированного носителя – уникальный.

3.4. Учетный номер наносится на машинный носитель персональных данных способом, обеспечивающим сохранность маркировки в процессе эксплуатации носителя и не приводящим его в негодность:

- учетный номер оптического носителя персональных данных наносится несмываемыми чернилами на его нерабочую поверхность и заверяется подписью администратора безопасности (на нерабочей стороне может указываться дополнительная информация, используемая в процессе применения);
- учетный номер жесткого диска наносится непосредственно на корпус носителя (при эксплуатации жесткого диска в составе СВТ, на корпус таких СВТ может наклеиваться этикетка с указанием количества и учетных номеров установленных в нем носителей информации);
- учетный номер флеш-памяти, ssd-дисков может наносится посредством специальной наклейки, номер заверяется подписью администратора безопасности.

4. Выдача машинных носителей персональных данных.

4.1. Работники получают учтенный машинный носитель персональных данных от администратора безопасности для выполнения работ на конкретный срок.

4.2. Выдача машинных носителей персональных данных работнику производится по Журналу учета машинных носителей персональных данных в Учреждении под подпись.

4.3. Выдача работникам съёмных машинных носителей персональных данных разрешается исключительно для реализации технологических процессов в ИСПДн, необходимых для выполнения трудовых (служебных) обязанностей, и осуществляется с оформлением Заявления на право использования съёмного машинного носителя информации по форме согласно *Приложение № 2 к настоящей Инструкции.*

4.4. По завершении работ или установленного срока использования работник сдает машинный носитель персональных данных администратору безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей персональных данных в Учреждении.

5. Использование и передача машинных носителей персональных данных.

5.1. На машинные носители персональных данных записываются исключительно ПДн и программные средства обработки ПДн, содержащиеся в ИСПДн.

5.2. Машинные носители персональных данных, допускающие повторную запись информации, при передаче между пользователями, в сторонние организации для ремонта или утилизации проходят процедуру уничтожения (стирания) персональных данных с оформлением Акта об уничтожении персональных данных в соответствии Положением о комиссии по уничтожению персональных данных в Учреждении с целью уничтожения остаточной информации.

Процедуру организует и контролирует администратор безопасности.

Акт об уничтожении персональных данных хранится у ответственного за организацию обработки ПДн.

5.3. Ремонт машинных носителей персональных данных, содержащие персональные данные, сторонней организацией запрещен.

5.4. ПДн, используемые в различных целях, записываются на разные машинные носители персональных данных.

5.5. Вынос машинных носителей персональных данных за пределы установленных мест обработки ПДн допустим только с письменного разрешения руководителя Учреждения.

5.6. Передача носителей, содержащих ПДн, которые обрабатываются в ИСПДн, сторонним организациям или третьим лицам производится по распоряжению руководителя Учреждения через администратора безопасности.

Администратор безопасности производит в этом случае необходимые отметки в Журнале учета машинных носителей персональных данных в Учреждении.

6. Хранение машинных носителей персональных данных

6.1. Хранение машинных носителей персональных данных осуществляется в условиях, препятствующих несанкционированному ознакомлению, копированию, изменению или уничтожению информации, содержащейся на машинных носителях.

6.2. Машинные носители персональных данных хранятся в служебных помещениях, съёмные машинные носители персональных данных - в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей.

В случае если на съёмном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

6.3. Хранение машинных носителей персональных данных осуществляется в условиях, исключающих утрату их функциональности и хранимой информации (оптические носители хранятся в конвертах или специальных коробках, обеспечивающих сохранность рабочей поверхности носителя от загрязнения и механических повреждений).

6.4. Порядок хранения машинных носителей персональных данных, предназначенных к списанию (уничтожению), в том числе нечитаемых вследствие выхода из строя из-за неисправности (износа), не изменяется.

6.5. Ответственным за сохранность машинного носителя персональных данных является пользователь ИСПДн, получивший машинный носитель персональных данных в соответствии с разделом 4 настоящей Инструкции.

7. Действия при выходе из строя, порче или утрате машинных носителей персональных данных.

7.1. В случае выхода из строя, утраты или порчи пользователем машинного носителя персональных данных немедленно ставится в известность администратор безопасности. Администратор безопасности докладывает об инциденте ответственному за организацию обработки ПДн.

7.2. Факт выхода из строя машинного носителя персональных данных устанавливается утвержденной приказом Учреждения комиссией (в состав комиссии включается администратор безопасности, системный администратор ИСПДн и ответственный за организацию обработки персональных данных) с оформлением Акта технической экспертизы состояния машинного носителя информации по форме согласно *Приложение № 3 к настоящей Инструкции*, утверждаемого руководителем Учреждения.

Неисправный носитель заменяется исправным, после чего администратором безопасности делаются соответствующие отметки в документах учета.

7.3. По факту утраты или порчи машинного носителя персональных данных, несанкционированного и (или) нецелевого использования учтенных машинных носителей информации проводится служебная проверка в установленном порядке по решению руководителя Учреждения.

Администратором безопасности делаются соответствующие отметки в документах учета.

7.4. Машинные носители персональных данных, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

8. Уничтожение машинных носителей персональных данных

8.1. Уничтожение машинных носителей персональных данных производится способом, гарантирующим невозможность восстановления информации, содержавшейся на носителе.

Такими способами являются: механическое, электрическое, электромагнитное, химическое или термическое воздействие на носитель, применение специального программного обеспечения для уничтожения информации на носителе.

Способ уничтожения выбирается администратором безопасности в зависимости от типа носителя и возможностей Учреждения.

8.2. Уничтожение машинных носителей персональных данных производится в присутствии членов комиссии, утвержденной распорядительным актом Учреждения «О создании комиссии по уничтожению персональных данных в Учреждении».

8.3. В случае проведения процедуры уничтожения машинного носителя информации сторонней организацией на основании заключенного гражданско-правового договора с учетом распорядительного акта Учреждения «О создании комиссии по уничтожению персональных данных в Учреждении» уничтожение машинного носителя информации оформляется Актом, который находится на хранении у администратора безопасности.

8.4. Утилизация лома уничтоженных носителей производится в соответствии с правилами уничтожения СВТ.

9. Контроль применения машинных носителей персональных данных

9.1. Контроль наличия машинных носителей персональных данных, правил и условий их хранения осуществляется посредством периодических проверок утвержденных распорядительным актом Учреждения комиссией, в состав которой включается ответственный за организацию обработки персональных данных и администратор безопасности.

Результаты проверки наличия машинных носителей персональных данных оформляются Актом проверки наличия и состояния машинных носителей информации по форме согласно *Приложению № 4 к настоящей инструкции.*

9.2. Проверке подлежат: соответствие количества учтенных носителей фактическому, наличие и состояние учетной документации, соответствие серийных (заводских) и учетных номеров, условия хранения и использования носителей.

9.3. Акт проверки хранится у администратора безопасности.

10. Ответственность

10.1. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией в соответствии с законодательством Российской Федерации.

Приложение № 1
к Инструкции по защите машинных носителей персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

Журнал учета машинных носителей персональных данных в Учреждении

Учетный № _____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№ п/п	Учетный (инвентарный) номер	Дата постановки на учет	Наименование, модель, емкость носителя	Заводской (серийный) номер	Тип носителя (съемный /несъемный)	Место установки (для несъемных носителей)	Ф.И.О. лица, эксплуатирующего носитель	Дата получения носителя и подпись	Дата возврата носителя и подпись администратора	Отметка об уничтожении носителя	Примечание
1	2	3	4	5	6	7	8	9	10	11	12
1	*инв. № 1000013*	*11.01.2021*	*USB flash drive Transcend JF V30/2Gb*	*81G1B77NBWB3F ACF&0*	*Съемный*	*нет*	*[И.О. Фамилия ответственного за организацию обработки ПДн]*	*01.01.2021 _____ [И.О. Фамилия ответственного за организацию обработки ПДн]*	*12.06.2021 _____ [И.О. Фамилия администратора безопасности]*	*уничтожен 20.06.2021*	

Лист _____

Правила
по формированию и ведению
журнала учета машинных носителей персональных данных
в Учреждении

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа - альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением листов титульного), нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны руководителем Учреждения с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – учетный порядковый номер записи;
- Графа 2 – учетный (инвентарный) номер носителя;
- Графа 3 – дата постановки на учет;
- Графа 4 – наименование, модель, емкость носителя;
- Графа 5 – заводской (серийный) номер носителя;
- Графа 6 – указывается тип носителя (съемный, несъёмный);
- Графа 7 – для несъемных носителей указывается АРМ пользователя.
- Графа 8 – Ф.И.О. работника
- Графа 9 – дата получения носителя и подпись пользователя;
- Графа 10 – дата возврата носителя и подпись администратора безопасности;
- Графа 11 – отметку делает администратор безопасности после уничтожения носителя;
- Графа 12 – любая информация, относящаяся к носителю.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

Приложение № 1
к Инструкции по защите машинных носителей персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

РАЗРЕШАЮ

Директор
ФИО
Наименование Учреждения

«___» _____ 20__ г.

Заявление
на право использования съёмного машинного носителя информации

Прошу разрешить для выполнения служебных (трудовых) обязанностей использование и подключение к АРМ (инв. № _____) съёмного машинного носителя персональных данных:

Должность	
ФИО полностью	
Цель использования в соответствии с служебными (трудовыми) обязанностями	
Технологический процесс, для реализации которого необходимо использование машинного носителя персональных данных	

Я предупрежден(а), что записывать, хранить на съёмных машинных носителях информации информацию ограниченного доступа допускается исключительно для реализации технологических процессов (регламентов, порядков работы и т.п.), необходимых для выполнения служебных (трудовых) обязанностей.

Подпись _____ /_____/

Дата _____

Согласовано:

Руководитель структурного подразделения _____/_____/

Выдан съёмный машинный носитель информации:

Учетный (регистрационный) № _____

Администратор безопасности _____/_____/

Приложение № 1
к Инструкции по защите машинных носителей персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

УТВЕРЖДАЮ

Директор
ФИО
Наименование Учреждения

«___» _____ 20__ г.

Акт № _____

технической экспертизы

состояния машинного носителя информации

г. _____ «____» _____ ____г.

Комиссия в составе:

Председатель комиссии:

_____
(должность. ФИО)

Члены комиссии: _____

(должность. ФИО)

_____
(должность. ФИО)

на основании _____

(приказ о назначении комиссии)

произвела наружный осмотр и контроль, сверила с данными регистрационного учета следующие носители информации:

№ п/п	Учетный (инвентарный) номер носителя	Наименование, модель, емкость носителя	Серийный (заводской) номер носителя	Место установки	Неисправность

в количестве _____ .
(количество цифрами и прописью)

В результате осмотра и контроля комиссия установила:

_____

(проявление неисправности, метод определения неработоспособности носителя информации)

_____

(возможность дальнейшего использования носителя информации, подлежит/не подлежит ремонту)

Характер записанной информации конфиденциальный, поэтому передача его в ремонт сторонней организации невозможна.

Заключение комиссии:

.

_____

(носитель информации подлежит /не подлежит утилизации)

Председатель комиссии:

_____ _____ _____

(должность) (подпись)

(ФИО)

Члены комиссии:

_____ _____ _____

(должность) (подпись)

(ФИО)

_____ _____ _____

(должность) (подпись)

(ФИО)

Приложение № 1
к Инструкции по защите машинных носителей персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

УТВЕРЖДАЮ

Директор
ФИО
Наименование Учреждения

Акт № _____
проверки наличия и состояния
машинных носителей информации

г. _____ «____» _____ ____г.

Комиссия в составе:

Председатель комиссии:

_____
(должность. ФИО)

Члены комиссии: _____

(должность. ФИО)

_____

на основании _____

(приказ о назначении комиссии)

провела проверку наличия и состояния машинных носителей информации в учреждении

Для проверки представлена следующая документация:
- Журнал учета носителей персональных данных в Учредении.

В соответствии с учетной документацией в учреждении числится:

1. Оптические диски в количестве ____ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание

2. Флеш – накопители в количестве ___ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание

3. Накопители на жестких дисках в количестве ___ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание

В ходе проверки выявлено:

_____

(соответствие/ не соответствие учетных носителей информации фактически представленному)

Заключение комиссии:

_____

(носители информации находятся в исправном/ неисправном состоянии, условия хранения и использования машинных носителей персональных данных соответствуют/ не соответствуют требованиях Инструкции по защите машинных носителей персональных данных в Учреждении)

Председатель комиссии:

_____ _____ _____

(должность) (подпись) (ФИО)

Члены комиссии:

_____ _____ _____

(должность) (подпись) (ФИО)

_____ _____ _____

(должность) (подпись) (ФИО)

Приложение № 4

УТВЕРЖДЕНО
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения.

1.1. Настоящее Положение об обеспечении безопасности персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Положение).

1.2. Настоящее Положение предназначено для применения при организации и проведении работ по обеспечению безопасности персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение).

1.3. Требования настоящего Положения распространяются на работников Учреждения, принимающих участие в обеспечении безопасности персональных данных в Учреждении. .

1.4. Положение определяет содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн) Учреждения, представляющей собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств.

1.5. В настоящем Положении использованы следующие сокращения:
- ИСПДн - информационная система персональных данных;
- НСД - несанкционированный доступ;
- ПДн - персональные данные;
- СКЗИ - средство криптографической защиты информации
- СЗПДн - система защиты персональных данных.

2. Термины и определения

2.1. В настоящем Положении 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.

- Вирус (компьютерный, программный): исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.
- 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.
- Защищаемая информация: информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
- Идентификация: присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- Информационная система персональных данных (ИСПДн): информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяюищих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таковых средств.
- Информационные технологии: процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.
- 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 персональных данных или других лиц либо иным образом, затрагивающих права и свободы субъекта персональных данных или других лиц.
- 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 персональных данных или наличия иного законного основания.
- Криптографическая защита: защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.
- Межсетевой экран: локальное (однокомпонентное) или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

- Недекларированные возможности: функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.
- Несанкционированный доступ (несанкционированные действия): доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.
- Обезличивание персональных данных: действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.
- 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 персональных данных.
- Оператор персональных данных (оператор): Учреждение, организующее и (или) осуществляющее обработку ПДн, а также определяющие цели и содержание обработки ПДн.
- Персональные данные (ПДн): любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).
- Предоставление информации: действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.
- Разграничение доступа (правила разграничения доступа): совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- Распространение персональных данных: действия, направленные на передачу ПДн определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.
- Средство вычислительной техники: совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
- Средство защиты информации: техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
- Технические средства информационной системы персональных данных: средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео - и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).
- Угрозы безопасности персональных данных: совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение,

блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

- Уничтожение персональных данных: действия, в результате которых невозможно восстановить содержание персональных данных в ИСПДн или в результате которых уничтожаются материальные носители персональных данных.
- Целостность информации: способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).
- Шифрование: процесс преобразования открытой информации с целью сохранения ее в тайне от посторонних лиц при помощи некоторого алгоритма, называемого шифром.
- Электронный документ: документ, в котором информация представлена в электронно-цифровой форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия.
- Электронная подпись: информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. .

3. Содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных.

3.1. Безопасность персональных данных при их обработке в ИСПДн достигается путем снижения вероятности осуществления НСД к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

3.2. При обработке персональных данных в ИСПДн Учреждением должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение НСД к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
- непрерывный контроль и анализ уровня защищенности персональных данных.

3.3. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные мероприятия и средства защиты информации (в том числе криптографические средства, средства предотвращения НСД, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПД информационные технологии..

3.4. Обеспечение безопасности персональных данных в Учреждении осуществляется на основе следующих принципов:

- соответствие мер и средств защиты актуальным угрозам безопасности - построение и модернизация СЗПДн в Учреждении производится на основе анализа угроз безопасности персональных данных с учетом специфических особенностей ИСПДн;
- соответствие мер и средств защиты требованиям нормативных документов РФ – в Учреждении используются меры и средства обеспечения безопасности персональных данных в строгом соответствии с действующими нормативными правовыми актами РФ в области обработки и защиты персональных данных;
- комплексность - с целью обеспечения безопасности персональных данных в Учреждении используется совокупность организационных мер и технических средств защиты;
- патентная чистота - средства защиты информации, входящие в состав СЗПДн, отвечают требованиям по обеспечению патентной чистоты согласно действующим нормативным документам РФ. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей.
- удобство пользователей - при построении и модернизации СЗПДн учитываются и по возможности сводятся к минимуму возможные трудности пользователей в работе со средствами защиты и с основными процедурами обеспечения безопасности персональных данных;
- постоянное совершенствование - осуществляется регулярный внутренний контроль выполнения требований по обработке и обеспечению безопасности персональных данных, эффективности применяемых организационных мер и технических средств защиты и уровня защищенности персональных данных, а также регулярно пересматриваются состав угроз и уровень защищенности ПДн, на основании чего принимаются меры по устранению выявленных недостатков и модернизации/совершенствованию СЗПДн..

3.5. Достаточность принятых мер по обеспечению безопасности персональных данных при обработке в ИСПДн оценивается при проведении внутреннего контроля.

3.6. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн Учреждения включают в себя:

- определение уровня защищенности обрабатываемых ПДн, в том числе отслеживание изменений состояния ИСПДн, которые могут повлиять на классификационные признаки ИСПДн (уровень защищенности ПДн);
- определение угроз безопасности персональных данных при их обработке в ИСПДН;
- разработка на основании определенных угроз и поддержание в актуальном состоянии частной модели безопасности угроз безопасности персональных данных при. обработке в ИСПДн;
- разработку на основе частной модели угроз системы защиты персональных данных (СЗПДн), обеспечивающей нейтрализацию предполагаемых поз с использованием методов и способов защиты персональных данных, предусмотренных для установленного уровня защищенности ПДн;
- установку и ввод в эксплуатацию СЗИ, входящих в состав СЗПДн, в соответствии с проектными решениями по созданию СЗПДн, эксплуатационной и технической документацией к данным СЗИ;
- обучение лиц, использующих СЗИ, входящие в состав СЗПДн, правилам работы с ними;
- учет применяемых СЗИ, входящих в состав СЗПДн, эксплуатационной и технической документации к ним;

- учет носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в ИСПДн;
- контроль соблюдения условий использования СЗИ, входящих в состав СЗПДн, предусмотренных эксплуатационной и технической документацией к ним;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования СЗИ, входящих в состав СЗПДн, которые могут привести к нарушению заданных характеристик безопасности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание состава и режима функционирования компонентов СЗПДн (описание СЗПДн).

3.7. Размещение компонентов ИСПДн, охрана помещений, в которых ведется работа с персональных данных, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и СЗИ, входящих в состав СЗПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

4. Внедрение организационных мер по обеспечению безопасности персональных данных.

4.1. В Учреждении утверждается и вводится в действие комплект организационно-распорядительной документации на СЗПДн.

4.2. Все должностные лица, допущенные к обработке персональных данных, и лица, ответственные за обеспечение безопасности персональных данных, в обязательном порядке изучают организационно-распорядительные документы на СЗПДн в части их касающейся и руководствуются ими в своей работе.

4.3. Общий контроль над исполнением требований организационно-распорядительной документации на СЗПДн в Учреждении возлагается на должностное лицо, ответственное за обеспечение безопасности ПДн.

5. Мероприятия по организации и обеспечению безопасности персональных данных.

5.1. Под организацией обеспечения безопасности персональных данных при их обработке в ИСПДн Учреждением понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени организационных и тематических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

5.2. В Учреждении определяются требования по обеспечению безопасности персональных данных на основании следующих документов:

- Акт определения уровня защищенности персональных данных при обработке в информационной системе персональных данных Учреждения по форме согласно *Приложению № 1 к настоящему Положению*;
- Акт оценки вреда, который может быть причинен субъектам персональных данных, персональные данные которых обрабатываются в информационной системе персональных данных Учреждения по форме согласно *Приложению № 2 к настоящему Положению*.

5.3. Организационные мероприятия по обеспечению безопасности персональных данных в Учреждении включает в себя:

- мероприятия по обеспечению охраны и физической защиты помещений, в которых расположены технические средства ИСПДн, исключающие несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности;
- обучение работников Учреждения правилам обработки и защиты персональных данных.

5.4. Для организации системы допуска и учета должностных лиц, допущенных к работе с персональными данными в Учреждении, должен быть определен перечень должностных лиц и утвержден соответствующим распорядительным актом Учреждения.

В Учреждении должна быть реализована разрешительная система допуска пользователей и разграничение прав доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации с помощью функциональных возможностей операционной системы, прикладных систем обработки персональных данных либо специализированных средств защиты информации.

Работникам Учреждения предоставляется доступ к ПДн и средствам их обработки в объеме, минимально необходимом для выполнения их трудовых обязанностей.Для идентификации и аутентификации пользователей ИСПДн Учреждением должны применяться пароли условно-постоянного действия.

5.5. Своевременное предоставление работникам Учреждения прав доступа к персональным данным и средствам их обработки, а также изменение их полномочий обеспечивает должностное лицо, ответственное за обеспечение безопасности ПДн в Учреждении.

Порядок генерации, смены и прекращения действия паролей в ИСПДн Учреждения определен в Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в Учреждении.

Приложение № 1
к Положению об обеспечении безопасности персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

АКТ
определения уровня защищённости персональных данных при их обработке в информационной системе персональных данных Учреждения

Ответственный в отношении организации обработки персональных данных в Учреждении _____

фамилия, имя, отчество, должность

с целью самостоятельной экспертной оценки необходимого уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных Учреждения, рассмотрев результаты по сбору и анализу исходных данных на информационные системы персональных данных, во исполнение требований: Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление Правительства № 1119); пункта 5 части 1 статьи 18.1 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных».

В соответствии с пунктом 7 Постановления Правительства № 1119 о том, что определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом проведенной оценки возможного вреда, определил:

- информационная система Учреждения является информационной системой, содержащей персональные данные.
- Тип обрабатываемых персональных данных принадлежит к категории «Иные».

В соответствии с пунктами 6, 7 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства № 1119 и актом оценки потенциального вреда субъектам персональных данных для информационной системы Учреждения актуальны угрозы безопасности персональных данных 3-го типа.

С учетом того, что число субъектов обрабатываемых персональных данных Менее 100 000, необходимо обеспечение 4-го уровня защищенности персональных данных при их обработке в информационной системе Учреждения.

По итогам определения уровня защищенности, необходимо принять меры в соответствии с Требованиями по защищенности для 4 уровня (в соответствии с Постановлением Правительства № 1119:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

«____» _____ 20___ г. _____

(подпись)

Приложение № 2
к Положению об обеспечении безопасности персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

АКТ
оценки вреда, который может быть причинен субъектам персональных данных, персональные данные которых обрабатываются в информационной системе персональных данных Учреждения

Оценка вреда производится с учетом требований Приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

Ответственный в отношении организации обработки персональных данных в Учреждении _____

фамилия, имя, отчество, должность

с целью самостоятельной экспертной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения в Учреждении обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, рассмотрев результаты по сбору и анализу исходных данных на информационные системы персональных данных, во исполнение требований пункта 5 части 1 статьи 18.1 Федерального закона № 152-ФЗ о том, что оператор персональных данных самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, и, в частности, к таким мерам относится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства в сфере персональных данных с учетом разработанных правил оценки вреда, который может быть причинен субъектам персональных данных, определил:

- инцидентов безопасности информации, связанных с нарушением Федерального закона № 152-ФЗ за предшествующие три года не было, в связи с чем коэффициент степени вероятности сценария инцидента устанавливается равным 1.
- Уровень вреда, который может быть причинен субъектам персональных данных в случае нарушения данного закона, оценивается как низкий в силу того, что Оператором не обрабатываются персональные данные, которые могут быть отнесены к специальным категориям персональных данных или которые являются биометрическими персональными данными.

Типы актуальных угроз безопасности ПДн	Оценки возможного вреда субъекту ПДн, определенные членами комиссии					Определение возможного вред (Y2)
	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Эксперт 5	
1	2	3	4	5	6	7
Кража ПЭВМ	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Y2=1,0 вред субъекта ПДн высокий
Кража носителей информации	Высокий (0,2)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2=0,5 вред субъекта ПДн низкий
Кража ключей и паролей доступа внутренними и внешними нарушителями	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Y2=1,0 вред субъекта ПДн высокий
Кража, модификация, уничтожение информации	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Y2=0,45 вред субъекта ПДн низкий

Вывод из строя узлов ПЭВМ, каналов связи	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Y2=0,2 вред субъекта ПДн нулевой
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Нулевой (0)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Y2=0,35 вред субъекта ПДн низкий
Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкий (0,05)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Y2=0,3 вред субъекта ПДн низкий
Непреднамеренное отключение средств защиты	Высокий (0,2)	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Y2=0,65 вред субъекта ПДн средний
Выход из строя аппаратно-программных средств	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2=0,3 вред субъекта ПДн низкий
Доступ к информации, модификация, в отношении лиц, не допущенных к обработке персональных данных	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2=0,9 вред субъекта ПДн средний
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Y2=0,8 вред субъекта ПДн средний
Несанкционированный доступ через ЛВС организации	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Y2=0,5 вред субъекта ПДн низкий
Несанкционированное отключение средств защиты	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2=0,6 вред субъекта ПДн средний
Действия вредоносных программ (вирусов)	Средний (0,1)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2=0,8 вред субъекта ПДн средний
Не декларированные возможности системного ПО и ПО для обработки персональных данных	Низкий (0,05)	Средний (0,1)	Высокий (0,2)	Низкий (0,05)	Низкий (0,05)	Y2=0,45 вред субъекта ПДн низкий
Установка ПО, не связанного с исполнением служебных обязательств	Нулевой (0)	Средний (0,1)	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Y2=0,2 вред субъекта ПДн нулевой
Внедрение аппаратных закладок	Нулевой (0)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2=0,3 вред субъекта ПДн низкий
Утрата паролей доступа к ИСПДН	Низкий (0,05)	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Y2=0,5 вред субъекта ПДн низкий
Перехват информации за пределами контролируемой зоны	Высокий (0,2)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Y2=0,55 вред субъекта ПДн средний
Удаленный запуск приложений	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Y2=0,5 вред субъекта ПДн низкий
Сканирование сети	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Нулевой (0)	Высокий (0,2)	Y2=0,4 вред субъекта ПДн низкий

На основании проведенной оценки уровня защищенности ИСПДн и категорий персональных данных, обрабатываемых в них, с учетом требований, предусмотренных статьями 18.1 и 19 Федерального закона № 152-ФЗ в Учреждении приняты следующие меры:

1. Назначен ответственный за обработку персональных данных и ответственный за обеспечение безопасности обработки персональных данных.
2. Осуществляется внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных.
3. Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.
4. Разработаны правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных.
5. Обеспечивается учет машинных носителей персональных данных.
6. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
7. Обеспечивается восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
8. Определен перечень работников, осуществляющих обработку персональных данных, сведения на бумажных носителях хранятся в сейфах или выделенных помещениях, определены места хранения персональных данных.
9. Ведется учет всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме).
10. Утверждены инструкции, регламентирующие работу с персональными данными и информационными системами персональных данных.

Принимаемые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, считать достаточными.

«____» _____ 20___ г. _____

(подписи)

Приложение № 5

УТВЕРЖДЕНЫ
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

ПРАВИЛА

рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Правила) определяют Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) порядок рассмотрения запросов субъектов персональных или их представителей.

1.2. В настоящих Правилах используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Иные термины, применяемые в настоящем Правилах, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты персональных данных.

Таблица 1 – Перечень сокращений

Сокращение	**Расшифровка сокращений**
ПДн	Персональные данные
Роскомнадзор	Уполномоченный орган по защите прав субъектов персональных данных
Федеральный закон № 152-ФЗ	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Таблица 2 – Перечень терминов и определений

Термин	**Определение**	**Источник**
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
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,	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»

Термин	Определение	Источник
	систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных	
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем	ГОСТ Р 50739-95

1.3. Настоящие Правила разработаны на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Трудового кодекса Российской Федерации.

1.4. Работники Учреждения, осуществляющие обработку персональных данных, должны быть ознакомлены с настоящими Правилами до начала обработки под подпись. Обязанность по организации ознакомления работников с настоящими Правилами возлагается на ответственного за организацию обработки ПДн в Учреждении (далее – ответственный за организацию обработки ПДн).

2. Правила рассмотрения запросов субъектов персональных данных

2.1. Организация приема и обработки обращений и запросов субъектов ПДн или их представителей, а также контроль за приемом и обработкой запросов возлагается на ответственного за организацию обработки ПДн.

2.2. Субъект ПДн имеет право на получение информации, в Учреждении касающейся обработки его ПДн (часть 7 статьи 14 Федерального закона № 152-ФЗ), в том числе содержащей:

- подтверждение факта обработки ПДн в Учреждении;
- правовые основания и цели обработки ПДн;
- цели и применяемые Учреждением способы обработки ПДн;
- наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения Учреждением обязанностей, установленных статьей 18.1 Федерального закона № 152-ФЗ;
- иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами Российской Федерации.

2.3. Сведения, указанные в пункте 2.2., должны предоставляться субъекту ПДн или его представителю Учреждением в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта ПДн или его представителя.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2.4. Запрос субъекта ПДн должен содержать:

- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения) либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;
- подпись субъекта ПДн или его представителя.

2.5. В Учреждении разработаны и используются соответствующие бланки с формами обращений субъектов ПДн согласно *Приложениям №1, №2, №3 и №4 к настоящим Правилам.*

2.6. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

2.7. Сведения, указанные в пункте 2.2, предоставляются Учреждением субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

2.8. Порядок направления субъектом ПДн повторного запроса в целях получения сведений, указанных в пункте 2.2, и его рассмотрения Учреждением определяется частями 4 - 6 статьи 14 Федерального закона № 152 – ФЗ.

2.9. Субъект ПДн вправе требовать от Учреждения уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2.10. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона № 152-ФЗ.

2.11. Запросы, поступающие в Учреждение, обрабатываются в соответствии с требованиями Федерального закона № 152-ФЗ и рассматриваются в соответствии с локальными актами Учреждения.

2.12. Все поступившие в Учреждение запросы регистрируются в день их поступления в Журнале учета обращений субъектов персональных данных или представителей субъектов ПДн, ведение которого определено в *Приложение № 5 к настоящим Правилам.* На запросе указывается входящий номер и дата регистрации.

2.13. Обязанность ведения Журнала учета обращений субъектов персональных данных или представителей субъектов персональных данных в Учреждении возлагается на работника соответствующим распоряжением Учреждения.

2.14. Рассмотрение запросов и подготовка ответов осуществляется по поручению руководителя Учреждения.

2.15. Работник Учреждения, осуществляющий обработку ПДн, в соответствии трудовыми (служебными) обязанностями, подготавливает проект ответа субъекту ПДн и визирует его у ответственного за организацию обработки ПДн.

2.16. Ответ субъекту ПДн направляется за подписью руководителя Учреждения.

2.17. Ответы субъекту ПДн направляются в виде уведомлений с использованием соответствующих форм бланков уведомлений согласно *Приложениям №6, №7, №8, №9, №10, №11 к настоящим Правилам.*

2.18. После отправки ответа на запрос осуществляется отметка в Журнале учета обращений субъектов персональных данных или представителей субъектов ПДн с указанием даты отправки.

2.19. Хранение запросов субъектов ПДн или их представителей и подготовленных ответов осуществляется не менее трех лет. Условия хранения указанных запросов и ответов должны препятствовать несанкционированному доступу до момента их уничтожения.

3. Ответственность

3.1. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами, в соответствии с законодательством Российской Федерации.

Приложение № 1
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Оператору персональных данных МУ «ВРМЦ»
Адрес: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99

Запрос на предоставление информации об обработке персональных данных

От _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____ № _____
(вид документа)

выдан _____
(кем и когда)

Адрес: _____

Сведения, подтверждающие факт обработки персональных данных в МУ «ВРМЦ»:
_____

В соответствии со статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» прошу предоставить мне следующую информацию, касающуюся обработки моих персональных данных:

- подтвердить факт обработки моих персональных данных;
- правовые основания и цели обработки моих персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и местонахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к моим персональным данным или которым могут быть раскрыты мои персональные данные на основании договора или на основании федерального закона;
- относящиеся ко мне обрабатываемые персональные данные, источник их получения;
- сроки обработки моих персональных данных, в том числе сроки их хранения;
- порядок осуществления мной прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или предполагаемой трансграничной передаче моих персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку моих персональных данных если обработка поручена или будет поручена такому лицу;
- информация о способах исполнения МУ «ВРМЦ» обязанностей, установленных статьей 18.1 Федерального закона № 152-ФЗ;
- _____.
(иные сведения)

Данный запрос является первичным / повторным, на основании того, что: _____
(ОБЯЗАТЕЛЬНО: указать причину направления повторного запроса)

Указанные сведения прошу предоставить по адресу: _____

_____ _____
(дата) (подпись)

Приложение № 2
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Оператору персональных данных МУ «ВРМЦ»
Адрес: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99

Запрос об отзыве согласия на обработку персональных данных

От _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____ № _____
(вид документа)

выдан _____
(кем и когда)

Адрес: _____

Сведения, подтверждающие факт обработки персональных данных в МУ «ВРМЦ»:

_____

Прошу прекратить обработку моих персональных данных, осуществляемую в целях:

_____
(цели обработки персональных данных, в отношении которых отзывается согласие)

по причине:

_____

_____ _____
(дата) (подпись)

Приложение № 3
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Оператору персональных данных МУ «ВРМЦ»
Адрес: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99

Запрос на уточнение персональных данных

От _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____ № _____
(вид документа)

выдан _____
(кем и когда)

Адрес: _____

Сведения, подтверждающие факт обработки персональных данных в МУ «ВРМЦ»:

_____

в соответствии с положениями статьями 14, 21 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» прошу уточнить/ уничтожить мои персональные данные в связи с тем, что:

_____

(указать причину: персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются

_____

необходимыми для заявленной цели обработки; с персональными данными, совершаются неправомерные действия – указать какие)

_____ _____
(дата) (подпись)

Приложение № 4
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Оператору персональных данных МУ «ВРМЦ»
Адрес: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99

Возражение
против принятия решений на основании исключительно автоматизированной обработки персональных данных

От _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____ № _____
(вид документа)

выдан _____
(кем и когда)

Адрес: _____

Сведения, подтверждающие факт обработки персональных данных в МУ «ВРМЦ»:
_____

Прошу исключить принятие в отношении меня юридически значимых решений на основании исключительно автоматизированной обработки моих персональных данных.

_____ _____
(дата) (подпись)

Приложение № 5
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Учетный № _____

Журнал

обращений субъектов персональных данных или представителей субъектов персональных данных в МУ «ВРМЦ»

Журнал начат _____

Журнал окончен _____

Листов (_____)

Лист _____

№	Сведения о запрашивающем лице (Ф.И.О., адрес)	Сведения о запросе			Сведения о принятом решении		Подпись ответственного лица	Примечание
		Дата поступления запроса	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации		
1	2	3	4	5	6	7	8	9
*1**	*Иванов И.И., РФ г. Иванов, ул. Иванова, д. 1, кв. 1*	*01.11.2021*	*перечень измененных персональных данных*	*уточнение персональных данных*	*отправлено почтовое уведомление №233 об уточнении ПДн*	*10.11.2021*	*_____ [И.О. Фамилия ответственного за организацию обработки ПДн]*	*Пример заполнения*

Правила
по формированию и ведению
журнала обращений субъектов персональных данных или представителей субъектов персональных данных в МУ "ВРМЦ"

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа – альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны руководителем МУ "ВРМЦ" с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – учетный порядковый номер записи;
- Графа 2 – Ф.И.О. и адрес субъекта ПДн, обратившегося в организацию по вопросу обработки его персональных данных;
- Графа 3 – дата поступления запроса;
- Графа 4 – кратко содержание обращения;
- Графа 5 – кратко о цели обращения субъекта ПДн;
- Графа 6 – запись о действии в ответ на обращение;
- Графа 7 – дата отправки уведомления субъекту ПДн;
- Графа 8 – подпись работника, отправившего уведомление субъекту ПДн.
- Графа 9 – любая информация, относящаяся к обращению субъекта ПДн.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.

Приложение № 6
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Субъекту персональных данных:
_____
_____
_____
(Ф.И.О.)

Адрес: _____
_____

Уведомление о прекращении обработки персональных данных

Оператор персональных данных: МУ «ВРМЦ», находящийся по адресу: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99, не осуществляет обработку Ваших персональных данных, начиная с:

_____
(дата, с которой прекращена обработка ПДН)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 7
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Субъекту персональных данных:
_____
_____
_____
(Ф.И.О.)
Адрес: _____
_____

Отказ в предоставлении сведений

Оператор персональных данных: МУ «ВРМЦ», находящийся по адресу: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99.

Вам отказано в предоставлении сведений по запросу от:

_____
(дата запроса)

на основании _____
(ссылка на нормы ФЗ РФ «О персональных данных» или иных федеральных законов)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 8
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Субъекту персональных данных:
_____
_____
_____
(Ф.И.О.)

Адрес: _____
_____

Уведомление о невозможности отзыва согласия на обработку персональных данных

Оператор персональных данных: МУ «ВРМЦ», находящийся по адресу: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99.

По Вашему запросу от _____
(дата запроса)
уведомляет Вас о невозможности отзыва согласия на обработку персональных данных в следующих целях: _____

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных: _____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 9
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Субъекту персональных данных:
_____
_____
_____
(Ф.И.О.)
Адрес: _____
_____

Уведомление об уточнении персональных данных

Оператор персональных данных: МУ «ВРМЦ», находящийся по адресу: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99.

По Вашему запросу от: _____,
(дата запроса)

было произведено уточнение Ваших персональных данных.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 10
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Субъекту персональных данных:
_____
_____
_____
(Ф.И.О.)

Адрес: _____
_____

Ответ
на возражение против принятия решений на основании исключительно автоматизированной обработки персональных данных

Оператор персональных данных: МУ "ВРМЦ", находящийся по адресу: 188640, Ленинградская обл, Всеволожский р-н, г Всеволожск, Колтушское шоссе, д 99,

рассмотрел Ваши возражения от: _____
(дата запроса)

И принял следующее решение:
_____
_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 11
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном учреждении «Всеволожский районный методический центр»

Субъекту персональных данных:
_____
_____
_____
(Ф.И.О.)
Адрес: _____
_____

Уведомление о блокировании персональных данных

Оператор персональных данных: МУ «ВРМЦ», находящийся по адресу: 188640, Ленинградская обл., Всеволожский р-н, г Всеволожск, Колтушское шоссе, д. 99, осуществил блокирование Ваших персональных данных, включая:

_____
(перечисление блокированных персональных данных: Ф.И.О., адрес, телефон)

которые обрабатывались в целях:

_____
(цель обработки указанных персональных данных)

Указанные персональные данные были заблокированы _____
(дата блокирования)

в связи с: _____
(причина блокирования персональных данных)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 6

УТВЕРЖДЕНЫ
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Правила) определяют в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) основания и порядок осуществления внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Политике Учреждения в отношении обработки персональных данных, локальным актам Учреждения.

1.2. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.3. Перечень нормативных правовых актов, на основании которых разработаны Правила:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – постановление Правительства РФ № 687);
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление Правительства РФ № 1119);
- приказ 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, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении

Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»»;

- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 №180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»;
- приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – приказ ФСТЭК России № 21);
- приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведении работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» (далее – приказ ФСТЭК России № 77).

1.4. Работники, допущенные к обработке персональных данных в Учреждении в связи с необходимостью выполнения ими трудовых (служебных) обязанностей, должны быть ознакомлены с настоящими Правилами под подпись до начала обработки персональных данных.

Обязанность по организации ознакомления указанных работников с настоящими Правилами возлагается на ответственного за организацию обработки персональных данных.

2. Основания проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2.1. Основаниями для проведения внутреннего контроля являются требования пункта 4 части 1 статьи 18.1., пункта 1 части 4, статьи 22.1. Федерального закона № 152-ФЗ, пункта 17 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ № 1119, ежегодный план внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных, утверждаемый руководителем Учреждения.

2.2. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) осуществляется в Учреждении путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов Учреждения по обработке и защите персональных данных.

2.3. Организация разработки проекта ежегодного плана внутренних проверок обеспечивается ответственным за организацию обработки персональных данных в Учреждении.

2.4. В случае проведения оценки соответствия информационной системы персональных данных требованиям по защите информации в форме аттестации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, обеспечивается проведение периодического контроля уровня защиты информации, результаты которого оформляются протоколами и отражаются в Техническом паспорте информационной системы персональных данных. Протоколы контроля защиты информации аттестованной информационной системы персональных данных не реже 1 раза в 2 года предоставляются в территориальный орган ФСТЭК России.

Непредставление протоколов контроля защиты информации в территориальный орган ФСТЭК России является основанием для приостановления действия аттестата соответствия информационной системы персональных данных требованиям по защите информации.

3. Порядок осуществления внутреннего контроля

3.1. Внутренний контроль проводится самостоятельно Учреждением и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.2. Для проведения внутреннего контроля в Учреждении создается комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Комиссия).

3.2.1. Состав Комиссии состоит из не менее трех работников Учреждения, утверждается распорядительным актом Учреждения.

Председателем Комиссии назначается ответственный за организацию обработки персональных данных в Учреждении.

В состав Комиссии также входят администратор безопасности информационной системы (систем) персональных данных в Учреждении.

Все члены комиссии при принятии решения обладают равными правами.

3.2.2. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных субъектов персональных данных.

3.3. Комиссия при проведении проверки обязана:

3.3.1. Провести анализ реализации мер, направленных на обеспечение выполнения Учреждением обязанностей, предусмотренных статьями 18.1, 19 Федерального закона № 152-ФЗ и принятыми в соответствии с ним локальными актами в отношении обработки персональных данных, и проверить:

- наличие актуального распорядительного акта Учреждения о назначении лица, ответственного за организацию обработки персональных данных в Учреждении, утвержденной инструкции ответственного за организацию обработки персональных данных в Учреждении, а также внесение соответствующих дополнений в трудовые (служебные) обязанности работника, назначенного ответственным за организацию обработки персональных данных в Учреждении;
- актуальность уведомления о намерении осуществлять обработку персональных данных, направленного в уполномоченный орган по защите прав субъектов персональных данных;
- актуальность Политики в отношении обработки персональных данных в Учреждении (далее - Политика) и обеспечение неограниченного доступа

к Политике и сведениям о реализуемых требованиях к защите персональных данных, в том числе размещение их на официальном сайте Учреждения в информационно-телекоммуникационной сети;

- наличие и актуальность Перечня персональных данных по каждой категории персональных данных, обрабатываемых в Учреждении, и Перечня информационных систем персональных данных в Учреждении;
- наличие правовых оснований для обработки персональных данных по каждой категории субъектов персональных данных, независимо от способа обработки персональных данных;
- соответствие целей обработки персональных данных содержанию и объему обрабатываемых персональных данных, независимо от способа их обработки;
- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ (далее – оценка вреда), соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения Учреждением обязанностей, предусмотренных Федеральным законом № 152-ФЗ. В случае необходимости по результатам проверки оценки вреда оформляется соответствующий акт;
- ознакомление работников (документально подтвержденное), непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки и обеспечения безопасности персональных данных;
- соответствие установленных прав доступа к персональным данным в информационной системе (системах) персональных данных трудовым (служебным) обязанностям работников Учреждения;
- наличие и полноту заполнения работниками Учреждения обязательств о соблюдении конфиденциальности персональных данных, документа об информировании о факте обработки персональных данных без использования средств автоматизации, разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- наличие согласий субъектов персональных данных на обработку персональных данных и разъяснений субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в случаях, когда этого требует законодательство Российской Федерации;
- наличие и ведение Журнала обращений субъектов персональных данных и представителей субъектов персональных данных, соблюдения процедур и сроков подготовки ответов на обращения субъектов персональных данных, а также учета предоставления персональных данных субъектов персональных данных по письменным запросам третьих лиц в порядке, установленном действующим законодательством Российской Федерации;
- наличие (в случае заключения соответствующего договора) в поручении на обработку персональных данных: перечня действия (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанности соблюдения конфиденциальности персональных данных, обеспечения безопасности

персональных данных при их обработке, а также требований к защите обрабатываемых персональных данных со статьей 19 Федерального закона № 152-ФЗ;

- актуальность Перечня мест хранения материальных носителей персональных данных и обеспечение контроля хранения материальных носителей персональных данных в условиях, исключающих несанкционированный доступ к ним, а также обеспечение раздельного хранения персональных данных в случаях их обработки без использования средств автоматизации при несовместимости целей обработки персональных данных;
- соблюдение сроков хранения и порядка уничтожения персональных данных в информационных системах персональных данных, материальных носителей персональных данных, а также персональных данных на носителях информации в соответствии с локальными актами Учреждения;
- актуальность организационно-распорядительных документов по вопросам обработки персональных данных.

3.3.2. Проанализировать выполнение в Учреждении требований по определению и обеспечению уровня защищенности персональных данных при их обработке в информационной системе персональных данных, утвержденных постановлением Правительства РФ № 1119, и проверить:

- соответствие указанных в утвержденном в Учреждении Перечне обрабатываемых персональных данных в информационной системе персональных данных категорий персональных данных, категорий субъектов персональных данных и количества субъектов персональных данных фактически обрабатываемым в информационной системе персональных данных;
- соответствие фактического типа актуальных угроз безопасности персональных данных в информационной системе персональных данных с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, типу актуальных угроз безопасности персональных данных, указанному в утвержденном руководителем Учреждении Акте классификации информационной системы персональных данных (в случае, если проводились работы по аттестации информационной системы персональных данных) либо в акте определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных (в случае, если работы по аттестации информационной системы персональных данных не проводились);
- назначение работника, ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;
- соответствие Перечня помещений, в которых размещена информационная система персональных данных, утвержденного в Учреждении, фактическому размещению оборудования информационной системы персональных данных, включая средства защиты информации;
- соответствие Перечня лиц, имеющих доступ к персональным данным в связи с исполнением своих трудовых (служебных) обязанностей Перечню лиц, имеющих доступ в помещения, в которых размещена информационная система персональных данных, утвержденного в Учреждении, фактически находящимся в указанных помещениях на момент проверки;

- фактическое выполнение организационных и технических мер по обеспечению безопасности помещений, в которых размещена информационная система персональных данных, препятствующих возможности неконтролируемого проникновения или пребывания в указанных помещениях лиц, не имеющих права доступа в них (при наличии - фактическое опечатывание входных дверей указанных помещений, применение систем контроля и управления доступом, средств охранной сигнализации, систем видеонаблюдения, оборудование оконных проемов первых и последних этажей здания, где размещено оборудование информационной системы персональных данных, запирающимися ставнями и т.д.);
- наличие сертификатов соответствия требованиям безопасности информации на все используемые средства защиты информации, фактически используемые в Учреждении;
- обеспечение сохранности машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные в информационной системе персональных данных путем проведения сверки соответствия количества учтенных носителей фактическому, а также сверки заводских и учетных номеров, фактической проверки условий хранения и использования машинных носителей персональных данных.

3.3.3. Проанализировать состояние работы в Учреждении по реализации Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России № 21 и проверить:

- фактическую реализацию установленного в Учреждении порядка идентификации и аутентификации пользователей информационной системы персональных данных;
- реализацию процесса управления доступом к ресурсам информационной системы персональных данных;
- регистрацию событий информационной безопасности в информационной системе персональных данных в соответствии с Инструкцией по управлению событиями информационной безопасности;
- реализацию выявления инцидентов информационной безопасности и реагирования на них при наличии запланированных работ по аттестации информационной системы персональных данных;
- организацию антивирусной защиты в информационной системе персональных данных и регулярность обновления базы данных признаков вредоносных программ (вирусов);
- реализацию выявления, анализа и устранения уязвимостей в информационной системе персональных данных при наличии запланированных работ по проведению аттестации информационной системы персональных данных;
- установку обновлений программного обеспечения, в том числе обновление программного обеспечения средств защиты информации;
- наличие проверок настройки правильности функционирования программного обеспечения и средств защиты информации в информационной системе персональных данных;

- организацию физического доступа к техническим средствам, средствам защиты информации информационной системы персональных данных, (в том числе опечатывание корпуса средств вычислительной техники);
- организацию размещения технических средств отображения информации информационных систем персональных данных, исключая ее несанкционированный просмотр;
- состав технических средств, программного обеспечения и средств защиты информации, входящих в состав информационной системы на соответствие Техническому паспорту информационной системы в случае, если запланировано проведение работ по аттестации информационной системы персональных данных;
- реализацию процесса управления конфигурацией информационной системы персональных данных и системы защиты персональных данных в случае, если запланировано проведение работ по аттестации информационной системы персональных данных.

3.4. Права комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

3.4.1. Комиссия при проведении проверки вправе:

- запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;
- получать в соответствии с Инструкцией пользователей информационной системы персональных данных временный доступ к ресурсам информационной системы персональных данных, в части касающейся ее полномочий;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;
- вносить руководителю Учреждения предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите персональных данных, установленных нормативными правовыми актами Российской Федерации.

3.4.2. При проведении проверки члены Комиссии не вправе:

- требовать представления документов и сведений, не относящихся к предмету проверки;
- распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

3.5. По результатам проверки составляется Акт проверки по форме согласно Приложению № 1 к настоящим Правилам, который подписывается всем составом комиссии и представляется руководителю Учреждения для принятия соответствующего решения.

В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты персональных данных, об их характере и о лицах, допустивших указанные нарушения.

Акт должен содержать заключение о соответствии или несоответствии обработки персональных данных требованиям к защите персональных данных и Политике Учреждения в отношении обработки персональных данных, установленным Федеральным законом № 152-ФЗ и принятыми в соответствии с ним

нормативными правовыми актами. Заключение о соответствии должно быть сформулировано для информационной системы персональных данных.

4. Ответственность

4.1. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами в соответствии с законодательством Российской Федерации.

Приложение № 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»»

Акт № _____
проведения внутренней проверки условий обработки персональных данных в Учреждении

Дата составления: «____» _____ 20____ г.
Место проведение проверки: _____

Комиссия, назначенная приказом руководителя от «___» _____ 20___ № ____
в составе:
Председатель: _____
(Ф.И.О.)
Члены комиссии:
_____
(Ф.И.О.)
_____
(Ф.И.О.)

руководствуясь «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, Политике Учреждения в отношении обработки персональных данных» провела проверку условий обработки персональных данных в Учреждении.

В ходе проверки:

- проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных статьями 18.1, 19 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним локальными актами Учреждения, определяющих его политику в отношении обработки персональных данных;
- проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных при их обработке в информационной системе персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- проведен анализ реализации в Учреждении организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- проведен анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы.

Выявленные нарушения: _____

ЗАКЛЮЧЕНИЕ комиссии:

Обработка персональных данных соответствует (не соответствует)

(нужное подчеркнуть)

требованиям к защите персональных данных и политике организации в отношении обработки персональных данных, установленным Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Председатель комиссии _____

(подпись)

Члены комиссии: _____

(подпись)

_____

(подпись)

Приложение № 7

УТВЕРЖДЕНА
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Инструкция ответственного за организацию обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения

1.1. Настоящая Инструкция ответственного за организацию обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее - Инструкция) определяет в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) обязанности и права работника, назначенного ответственным за организацию обработки персональных данных.

1.2. Настоящая Инструкция разработана на основании следующих нормативных правовых актов:

- Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению удаления персональных данных»;
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»;

– приказ Федеральной службы безопасности Российской Федерации от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».

1.3. При назначении работника Учреждения ответственным за организацию обработки ПДн его должностная инструкция дополняется правами и обязанностями, предусмотренными настоящей Инструкцией, с соблюдением положений действующего законодательства Российской Федерации.

1.4. В своей деятельности ответственный за организацию обработки ПДн руководствуется законодательством Российской Федерации, локальными актами Учреждения, относящимися к обработке и защите ПДн, а также настоящей Инструкцией.

1.5. В Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращений
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - уполномоченный орган по защите прав субъектов персональных данных
ФАПСИ	Федеральное агентство правительственной связи и информации при Президенте Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Администратор безопасности	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе	постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Безопасность информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	ГОСТ Р 50922-2006
Доступность	Состояние информации (ресурсов	Р 50.1.056-2005

информации (ресурсов информационной системы)	автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно	
Защита информации	Состояние защищенности информации (данных), при котором обеспечены ее их (конфиденциальность, доступность и целостность)	ГОСТ Р 50922-2006
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов	Федеральный закон Российской Федерации от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Контролируемая зона	Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств.	ГОСТ Р 56115-2014
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя	Федеральный закон Российской Федерации от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
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	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Система защиты информации	Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и	ГОСТ Р 50922-2006

	функционирующая по правилам и нормам, установленными соответствующими документами в области защиты информации	
Событие информационной безопасности	Выявленное состояние системы, услуги или состояние сети, указывающее на возможное нарушение политики обеспечения информационной безопасности, нарушение или отказ мер и средств контроля и управления или прежде неизвестная ситуация, которая может иметь значение для безопасности	ГОСТ Р ИСО/МЭК 27000-2012
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем	ГОСТ Р 50739-95
Средства криптографической защиты информации	Шифровальные (криптографические) средства защиты информации конфиденциального характера К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	Приказ ФАПСИ от 13.06.2001 № 152
Уязвимость	Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть	ГОСТ Р 56545-2015

	использована для реализации угроз безопасности информации	
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право	Р 50.1.056-2005
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

1.6. Ответственный за организацию обработки ПДн включается в состав комиссии по определению уровня защищенности ПДн при их обработке в ИСПДн, утверждаемой распорядительным актом Учреждения.

1.7. Ответственный за организацию обработки ПДн осуществляет методическое руководство деятельностью администратора безопасности.

1.8. С настоящей Инструкцией и дополненной должностной инструкцией ответственный за организацию обработки ПДн знакомится под подпись.

2. Обязанности ответственного за организацию обработки персональных данных

2.1. Ответственный за организацию обработки ПДн обязан знать:

- и выполнять требования законодательства Российской Федерации и локальных актов Учреждения, устанавливающих правила обработки и защиты ПДн;
- цели обработки ПДн в Учреждении и перечень, обрабатываемых ПДн в ИСПДн, а также обрабатываемых без использования средств автоматизации;

2.2. Ответственный за организацию обработки ПДн обязан обеспечивать:

- взаимодействие с Роскомнадзором в соответствии с Порядком взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в Учреждении согласно *Приложению № 1 к настоящей Инструкции; в том числе:*
  - по своевременному направлению в территориальный орган по защите прав субъектов ПДн уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных;
  - в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн;

2.3. Ответственный за организацию обработки ПДн обязан организовывать и осуществлять:

- взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, о компьютерных инцидентах, повлекших неправомерную передачу

(предоставление, распространение, доступ) персональных данных, в порядке, определенном указанным федеральным органом исполнительной власти;

- оценку вреда, который может быть причинен субъектам персональных данных, персональные данные которых обрабатываются в Учреждении (далее – оценка вреда). По результатам оценки вреда составлять соответствующий акт по форме согласно *Приложению № 2 к настоящей Инструкции*;
- размещение на официальном сайте Учреждения «Политики в отношении обработки персональных данных в Учреждении», а также обеспечивать её актуализацию;
- ведение перечня работников Учреждения, доступ которых к ПДн, обрабатываемым в ИСПДн и без использования средств автоматизации, необходим для выполнения ими трудовых (служебных) обязанностей;
- поддержание в актуальном состоянии перечня ПДн, обрабатываемых в ИСПДн в Учреждении;
- режим обеспечения безопасности помещений, в которых размещены средства вычислительной техники ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, а также осуществлять периодическую проверку состояния физической защиты ИСПДн (средства охраны и физического доступа в контролируемых зонах ИСПДн);
- актуальность перечня помещений в Учреждении, в которых осуществляется обработка ПДн и размещены средства вычислительной техники ИСПДн;

2.4. Ответственный за организацию обработки ПДн:

- в случае необходимости вносит предложения руководителю Учреждения по обеспечению антивирусной защиты в ИСПДн;
- контролирует изменения в конфигурации ИСПДн и оценивать возможный вред, который может быть причинен субъектам ПДн в результате указанных изменений, а также организовывать работы по восстановлению конфигурации ИСПДн и системы защиты информации;
- обеспечивает контроль за организацией и проведением мероприятий по выявлению (поиску), анализу и устранению уязвимостей в ИСПДн, а также внеплановых процедур выявления (поиска) анализа и устранения уязвимостей на основе анализа журналов событий информационной безопасности;
- контролирует уровень защищенности ПДн, обрабатываемых в ИСПДн и организовывать мероприятия по доработке системы защиты информации с целью обеспечения установленного для ИСПДн уровня защищенности ПДн;
- рассматривает предложения администратора безопасности по совершенствованию действующей системы защиты ПДн в Учреждении;
- в случае необходимости инициирует перед руководителем Учреждения пересмотр ранее установленного уровня защищенности ПДн при их обработке в ИСПДн;
- организовывает проведение мероприятий по заключению договоров на работы по защите ПДн;
- доводит до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывает обучение и контроль знаний работников, осуществляющих обработку ПДн в ИСПДн, а также без использования средств автоматизации,

в области защиты и обработки ПДн с письменным подтверждением проведения указанных мероприятий;

- обеспечивает своевременное выполнение работниками Учреждения требований действующего законодательства Российской Федерации, а также нормативных актов Учреждения в сфере обработки и обеспечения безопасности персональных данных;
- организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- осуществляет внутренний контроль за соблюдением работниками норм действующего законодательства Российской Федерации в сфере обработки и обеспечения безопасности ПДн. Результаты внутреннего контроля докладываются руководителю Учреждения;
- инициирует не реже 1 раза в 3 года контроль за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- инициирует не реже 1 раза в год проведение проверки наличия средств криптографической защиты информации, эксплуатационной и технической документации к ним, соблюдения условий использования средств криптографической защиты информации.

3. Права.

3.1. Ответственный за организацию обработки ПДн имеет право:

- знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него обязанностей;
- подготавливать предложения руководителю Учреждения по защите ПДн, обрабатываемых в ИСПДн, и обеспечения работ по организации обработки ПДн;
- разрабатывать проекты организационно-распорядительных документов (приказы, распоряжения) Учреждения по защите ПДн, обрабатываемых в ИСПДн, и организации обработки ПДн в целом;
- проводить проверки соблюдения режима обеспечения безопасности ПДн в структурных подразделениях Учреждения;
- требовать от работников соблюдения требований действующего законодательства Российской Федерации в сфере обработки и обеспечения безопасности, а также требований, установленных организационно-распорядительной документацией по защите ПДн Учреждения;
- вносить предложения руководителю Учреждения о привлечении к дисциплинарной ответственности работников, систематически нарушающих требования по обработке и защите ПДн;
- давать работникам Учреждения обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и локальными актами Учреждения.

Приложение № 1
к Инструкции ответственного за организацию обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения

1.1. Настоящий Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее - Порядок) определяет порядок действий Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) по выполнению положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» при взаимодействии с уполномоченным органом защите прав субъектов персональных данных (далее - Роскомнадзор).

1.2. В настоящем Порядке используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно. Иные термины, применяемые в настоящем Порядке, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты персональных данных.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращений
ЕСИА	Единая система идентификации и аутентификации
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
Федеральный закон № 152-ФЗ	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон № 152-ФЗ
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон № 152-ФЗ
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,	Федеральный закон № 152-ФЗ

Термин	Определение	Источник
	доступ), обезличивание, блокирование, удаление, уничтожение персональных данных	
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон № 152-ФЗ
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон № 152-ФЗ

1.3. Работники Учреждения, осуществляющие обработку персональных данных, должны быть ознакомлены с настоящим Порядком до начала обработки под подпись. Обязанность по организации ознакомления работников с настоящим Порядком возлагается на ответственного за организацию обработки ПДн в Учреждении (далее – ответственный за организацию обработки ПДн).

1.4. Обязанность по организации выполнения требований данного Порядка возлагается на ответственного за организацию обработки ПДн.

1.5. Учреждение вправе осуществлять без уведомления территориального органа Роскомнадзора обработку персональных данных (далее - ПДн) в случае, если Учреждение осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации.

2. Порядок действий ответственного за организацию обработки ПДн

2.1. Перед началом обработки персональных данных ответственный за организацию ПДн обеспечивает уведомление территориального органа

Роскомнадзора по месту нахождения Учреждения о намерении Учреждения осуществлять обработку ПДн.

2.2. В случае изменения сведений, указанных в уведомлении о намерении осуществлять обработку ПДн, ответственный за организацию обработки не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения, организует направление в территориальный орган Роскомнадзора уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку ПДн.

2.3. В случае прекращения обработки ПДн ответственный за организацию обработки ПДн организует направление в территориальный орган Роскомнадзора уведомления о прекращении обработки ПДн, в срок, не превышающий 10 рабочих дней с даты прекращения обработки ПДн.

2.4. Если из территориального органа Роскомнадзора поступил запрос о предоставлении информации, то ответственный за организацию обработки ПДн в течение **10 рабочих дней** с момента получения запроса из территориального органа Роскомнадзора формирует и организует направление ответа на запрос. Указанный срок может быть продлен, но не более чем на **5 рабочих дней** в случае направления ответственным за организацию обработки ПДн в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2.5. Полученные запросы уполномоченного органа по защите прав субъектов ПДн регистрируются ответственным за организацию обработки ПДн в Журнале учета запросов уполномоченного органа по защите прав субъектов ПДн.

2.6. При получении правомерного запроса из территориального органа Роскомнадзора на исправление выявленных нарушений ответственный за организацию обработки ПДн организует силами администраторов безопасности ИСПДн, администраторов ИСПДн, в которых обрабатываются указанные ПДн, разработку перечня действий по устранению выявленных нарушений и обеспечивает его согласование с заинтересованными подразделениями Учреждения.

Устранение выявленных нарушений осуществляется в срок, не превышающий **3 рабочих дней** со дня выявления нарушений.

По факту устранения нарушений уведомляется территориальный орган Роскомнадзора через регистрируемое почтовое отправление с заказным уведомлением о вручении.

Контроль за своевременным уведомлением территориального органа Роскомнадзора возлагается на ответственного за организацию обработки ПДн.

2.7. Уведомление об устранении нарушений в порядке обработки ПДн. ответственный за организацию обработки ПДн регистрирует в Журнале учета запросов уполномоченного органа по защите прав субъектов ПДн.

2.8. В случае, если обеспечить правомерность обработки ПДн невозможно, то ответственный за организацию обработки ПДн оформляет служебную записку на имя руководителя Учреждения о необходимости уничтожения ПДн.

Уничтожение ПДн осуществляется комиссией Учреждения по уничтожению персональных данных в Учреждении в срок, не превышающий **10 рабочих дней** с даты выявления неправомерной обработки ПДн.

По факту уничтожения ПДн составляется акт об уничтожении персональных данных в соответствии с Положением о комиссии Учреждения по уничтожению

персональных данных, а также обеспечивается выгрузка из журнала регистрации событий в соответствующей информационной системе персональных данных (при наличии).

Об уничтожении указанных ПДн уведомляется территориальный орган Роскомнадзора в порядке, установленном пунктом 2.6 настоящей Инструкции.

2.9. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, ответственный за организацию обработки ПДн с момента выявления такого инцидента Учреждением, уполномоченным органом по защите прав субъектов ПДн или иным заинтересованным лицом уведомляет территориальный орган Роскомнадзора:

- в течение **24 часов** о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном Учреждением на взаимодействие с территориальным органом Роскомнадзора, по вопросам, связанным с выявленным инцидентом;
- в течение **72 часов** о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

2.10. В случае, если территориальным органом Роскомнадзора осуществлялась выездная проверка, то по её окончании должностное лицо территориального органа Роскомнадзора производит запись о проведенной проверке в журнале учета проверок.

2.11. Форма журнала регламентирована приказом министерства экономического развития Российской Федерации от 30.04.2009 № 141 «О реализации положений Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

Ведение указанного журнала обеспечивает ответственный за организацию обработки ПДн.

3. Взаимодействие с территориальным органом с использованием информационно-телекоммуникационной сети Интернет

3.1. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является дополнительным средством для обеспечения возможности обращений граждан объединений граждан и юридических лиц в Роскомнадзор.

3.2. Для подготовки и отправки уведомления о намерении осуществлять обработку персональных данных либо уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных (далее – информационное письмо) необходимо перейти на официальный сайт Роскомнадзора в информационно-телекоммуникационной сети Интернет.

3.3. Для отправки уведомления либо информационного письма требуется выбрать один из трех способов заполнения и направления уведомления, либо информационного письма в территориальный орган Роскомнадзора:

- сформировать уведомление либо информационное письмо и направить его в бумажном виде;

- сформировать уведомление и направить в электронном виде с использованием усиленной квалифицированной электронной подписи;
- сформировать уведомление и направить в электронном виде с использованием средств аутентификации ЕСИА.

3.4. В случае выбора способа направления уведомления либо информационного письма в Роскомнадзор в бумажном виде и после открытия соответствующей формы, следует её заполнить и отправить в информационную систему Роскомнадзора, а затем распечатать заполненную форму на бланке письма Учреждения, подписать её у руководителя Учреждения, поставить печать Учреждения и направить в соответствующий территориальный орган Роскомнадзора по месту нахождения Учреждения нарочным под подпись о получении сотрудником территориального органа Роскомнадзора.

3.5. В случаях, если форма подписывается усиленной квалифицированной электронной подписью либо направляется в электронном виде с использованием средств аутентификации ЕСИА (**esia.gosuslugi.ru**), то её дальнейшее направление на бумажном носителе в территориальный орган Роскомнадзора не требуется.

3.6. При выборе способа направления формы с использованием усиленной квалифицированной электронной подписи необходим плагин КриптоПро ЭЦП Browser plug-in и настроена работа с ним.

3.7. В случае выбора способа направления формы в электронном виде с использованием средств аутентификации ЕСИА требуется пройти аутентификацию на портале Государственных услуг, заполнить форму и направить ее в электронном виде. При этом уже должна иметься подтвержденная учетная запись, привязанная к Учреждению на портале Государственных услуг.

4. Ответственность

4.1. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 2
к Инструкции ответственного за организацию обработки персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

УТВЕРЖДАЮ
Учреждение
Руководитель
ФИО

_____
(подпись, печать)

«____» _____ 20____ г.

АКТ

оценки вреда, который может быть причинен субъектам персональных данных, персональные данные которых обрабатываются в информационной системе персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

В соответствии с приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» в целях реализации пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон) мною, ответственным за организацию обработки персональных данных в Учреждении _____
(ФИО, должность ответственного за организацию обработки персональных данных)
осуществлена оценка вреда, который может быть причинен субъектам персональных данных, персональные данные которых обрабатываются в информационной системе персональных данных Учреждения, в случае нарушения Федерального закона «О персональных данных» (далее – оценка вреда).

В результате осуществленной «____» _____ 20___ года оценки вреда на основании подпунктов 2.1-2.3 пункта 2 Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», утвержденных приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»» установлена _____ степень вреда, который может быть
(высокая, средняя, низкая, отсутствует)
причинен субъектам персональных данных, персональные данные которых обрабатываются в информационной системе персональных данных Учреждения.

«____» _____ 20___ г. _____
(подпись)

Приложение № 8

УТВЕРЖДЕНА
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения

1.1. Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – администратор безопасности) определяет в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) обязанности, права и ответственность работника, назначенного администратором безопасности.

1.2. В своей деятельности администратор безопасности руководствуется законодательством Российской Федерации, иными нормативными правовыми актами Российской Федерации в сфере обработки и защиты персональных данных, локальными актами Учреждения, а также настоящей Инструкцией.

1.3. Администратор безопасности назначается распорядительным актом Учреждения и обеспечивает в пределах своих трудовых (служебных) обязанностей безопасность персональных данных, обрабатываемых в информационных системах персональных данных (далее – ИСПДн) в Учреждении.

2. Обязанности администратора безопасности

2.1. Администратор безопасности при эксплуатации ИСПДн обязан:

- соблюдать требования законодательных и нормативных документов по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;
- выполнять и принимать меры к выполнению требований организационно-распорядительной документации по организации обработки и защиты персональных данных в ИСПДн;

2.2. Администратор безопасности при эксплуатации ИСПДн обязан осуществлять:

- установку, настройку и сопровождение технических средств защиты ИСПДн;
- организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов и паролей доступа в ИСПДн;
- контроль действий пользователей ИСПДн при их работе с персональными идентификаторами и паролями доступа:
  - создавать, присваивать, уничтожать персональные идентификаторы и пароли доступа к техническим средствам и информационным ресурсам ИСПДн;
  - хранить, выдавать, инициализировать, блокировать средства аутентификации (пароли, аппаратные идентификаторы) и принимать меры в случае утраты или компрометации средств аутентификации;
  - вести, надежно хранить и в установленном порядке уничтожать Журналы учета выдачи первичных паролей информационных систем персональных данных;

- обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 90 дней с момента очередной смены и изменять свой собственный пароль не реже 1 раза в месяц. Принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере индивидуальных аппаратных идентификаторов;

2.3. Администратор безопасности при эксплуатации ИСПДн обязан надежно хранить:

- и вести учет аппаратных средств аутентификации по Журналу учета аппаратных средств аутентификации Учреждения;
- и в установленном порядке уничтожать Журнал учета аппаратных средств аутентификации Учреждения;

2.4. Администратор безопасности при эксплуатации ИСПДн обязан:

- сообщать ответственному за организацию обработки персональных данных в Учреждении об инцидентах, связанных с компрометацией или утерей паролей, аппаратных идентификаторов;
- выявлять и пресекать действия пользователей, которые могут привести к компрометации паролей и (или) утрате аппаратных идентификаторов.
- осуществлять и контролировать разграничение доступа пользователей к ресурсам и персональным данным, обрабатываемым в ИСПДн, путем настройки программно-технических средств и средств защиты информации:
  - управлять учетными записями (заведение, активацию, блокирование, уничтожение), в том числе осуществлять блокирование учетной записи при превышении времени неиспользования более 90 дней, в случае достижения установленного максимального количества неуспешных попыток аутентификации в течение не более 30 минут (максимальное количество неуспешных попыток аутентификации до блокировки до 5 попыток), блокирование сеанса доступа в ИСПДн после установленного времени бездействия (неактивности) пользователя 30 минут или по его запросу;
  - обеспечивать актуальность, сохранность и конфиденциальность матриц доступа к ресурсам ИСПДн, утвержденных распорядительным актом Учреждения;

2.5. Администратор безопасности при эксплуатации ИСПДн обязан вести учет:

- технических средств удаленного доступа (в случае использования удаленного доступа через сеть Интернет к ресурсам ИСПДн) с документальным оформлением в Журнале учета разрешенных средств удаленного доступа в Учреждении, а также осуществлять выдачу, хранение технических средств удаленного доступа, установку и настройку программного обеспечения, его обновление, антивирусную защиту технических средств удаленного доступа и контролировать использование технических средств удаленного доступа к ИСПДн;
- мобильных технических средств (в случае использования мобильных технических средств для доступа к ресурсам ИСПДн) с документальным оформлением в Журнале учета разрешенных мобильных технических средств в Учреждении и контролировать использование мобильных технических средств для доступа к ИСПДн.
- хранение и выдачу машинных носителей персональных данных, в том числе:
  - организовывать и контролировать процедуру уничтожения (стирания) или обезличивания персональных данных при передаче между пользователями,

в сторонние организации для ремонта или утилизации, а также факт уничтожения машинного носителя персональных данных;
- участвовать в составе комиссии по проверке наличия и состояния машинных носителей персональных данных;
- в случае выхода из строя, порчи или утраты машинного носителя персональных данных докладывать об инциденте ответственному за организацию обработки персональных данных в Учреждении.

2.6. Администратор безопасности при эксплуатации ИСПДн обязан:

- контролировать проведение резервного копирования технических средств ИСПДн (при организации).
- осуществлять настройку журналов регистрации событий информационной безопасности в программном обеспечении ИСПДн и средств защиты информации в части касающейся, фиксировать информацию о событиях безопасности в информационных системах, не подлежащую автоматической регистрации в Журнале событий информационной безопасности информационной системы персональных данных.
- вести, надежно хранить Журнал событий информационной безопасности информационной системы персональных данных;
- осуществлять установку, конфигурирование и управление средствами антивирусной защиты ИСПДн, в том числе:
  - установку и обновление лицензионных ключей средств антивирусной защиты, обновлений базы признаков вредоносных компьютерных программ (вирусов);
  - принимать меры по локализации и удалению вредоносного программного обеспечения, выявлению источника и способа проникновения вредоносного программного обеспечения;
  - восстановление работоспособности программных средств и информационных массивов программных средств, поврежденных вредоносным программным обеспечением;
  - ограничение доступа пользователей на автоматизированным рабочих местах (далее - АРМ) к настройкам установленных средств антивирусной защиты;
  - контроль над работой пользователей ИСПДн по применению на непосредственных АРМ средств антивирусной защиты,
  - немедленно оповещать ответственного за организацию обработки персональных данных в Учреждении об обнаружении вредоносного программного обеспечения на серверном или телекоммуникационном оборудовании.
- осуществлять исполнение мероприятий по выявлению (поиску), анализу и устранению уязвимостей в ИСПДн (с разработкой Плана устранения выявленных уязвимостей):
  - осуществлять мониторинг наличия обновлений, выпускаемых разработчиками программного обеспечения, используемого в ИСПДн и средствах защиты информации, в части касающейся;
  - проводить обновление программного обеспечения средств защиты информации, программного обеспечения программно-аппаратных средств в случае выявления уязвимостей, связанных с устаревшими версиями программного обеспечения;

- выполнять необходимые настройки, проводить тестирование работоспособности после установки обновлений программного обеспечения и вносить необходимые изменения в эксплуатационную документацию;
- проводить контроль установки обновлений программного обеспечения (проводить проверку соответствия версии общесистемного, прикладного и специального программного обеспечения, установленного в ИСПДн, а также программного обеспечения средств защиты информации, выпущенного разработчиком, наличия соответствующих отметок в Техническом паспорте и в эксплуатационной документации);
- не реже 1 раза в полгода проводить контроль на соответствие Техническим паспортам ИСПДн состава технических средств, программного обеспечения и средств защиты информации.
- осуществлять проверку наличия и сроков действия лицензий на установленное программное обеспечение ИСПДн и программное обеспечение средств защиты информации, сертификатов соответствия на примененные в ИСПДн и средствах защиты информации программно-аппаратных средств;
- ежемесячно проводить контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- немедленно уведомлять ответственного за организацию обработки персональных данных в Учреждении при получении информации о прекращении поддержки разработчиком используемого программного обеспечения в части выпуска обновлений безопасности, либо о планируемом прекращении такой поддержки;
- проводить проверку технического состояния аппаратных средств, журналов планово-профилактического обслуживания аппаратных средств ИСПДн за период контроля защищенности ИСПДн, перечня событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств, конфигурацию соединений и установки аппаратных средств, условия их эксплуатации;
- осуществлять контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации, в случае выявления сбоев, отказов или несоответствия настройкам, организовывать восстановление программного обеспечения и средств защиты информации;
- участвовать в организованной ответственным за организацию обработки персональных данных в Учреждении проверке состояния и актуальности организационно-распорядительной документации по защите персональных данных, обрабатываемых в ИСПДн.

- проводить анализ планируемых изменений в конфигурацию ИСПДн и системы защиты персональных данных, отнесенным к 3 уровню защищенности персональных данных при их обработке в ИСПДн, и принимать решение о необходимости внесения изменения в конфигурацию ИСПДн и системы защиты персональных данных, осуществлять проверку корректности изменения конфигурации и при необходимости совместно с ответственным за организацию обработки персональных данных в Учреждении организовать актуализацию документации по вопросам обеспечения безопасности персональных данных при

их обработке в ИСПДн, а также контроль эффективности обеспечения безопасности персональных данных при их обработке в ИСПДн.

- контролировать выполнение требований к размещению устройств вывода информации в контролируемых зонах, расположение технических устройств и физический доступ к ним.

3. Права администратора безопасности

3.1. Администратор безопасности имеет право:

- привлекать к работам, связанным с обеспечением безопасности персональных данных в ИСПДн системных администраторов ИСПДн;
- требовать от пользователей ИСПДн выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности ИСПДн;
- докладывать ответственному за организацию обработки персональных данных в Учреждении о нарушениях или невыполнении пользователями требований обеспечению безопасности персональных данных;
- вносить предложения по модернизации и совершенствованию систем защиты персональных данных в Учреждении ответственному за организацию обработки персональных данных в Учреждении;
- останавливать обработку персональных данных в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования средств защиты информации.

4. Ответственность.

4.1. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 9

УТВЕРЖДЕН
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Перечень лиц, имеющих доступ к персональными данными работников МУ «ВРМЦ» в связи с исполнением своих трудовых (служебных) обязанностей

№ п/п	Фамилия, имя, отчество	Должность
1.	Долгобородова Любовь Егоровна	главный бухгалтер
2.	Абрамова Ирина Григорьевна	Специалист по закупкам
3.	Куракина Наталья Владимировна	документовед
4.	Николаев Алексей Евгеньевич	инженер-программист (программист)
5.	Созонова Вера Александровна	бухгалтер
6.	Федотова Евгения Алексеевна	методист

Приложение № 10

УТВЕРЖДЕНА
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Инструкция пользователя информационных систем персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения

1.1. Настоящая Инструкция пользователя информационных систем персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Инструкция) определяет в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) обязанности, права и ответственность пользователей информационных систем персональных данных (далее – информационные системы).

1.2. Пользователями информационных систем являются работники Учреждения, допущенные к обработке персональных данных в информационных системах в соответствии с утвержденным в Учреждении перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационных системе персональных в Учреждении необходим для выполнения ими трудовых (служебных) обязанностей.

1.3. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
АРМ	Автоматизированное рабочее место
ПДн	Персональные данные
СВТ	Средства вычислительной техники
ПО	Программное обеспечение

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в ин формационной системе персональных данных	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Машинный носитель	Материальный носитель, используемый для	

Термин	Определение	Источник
информации	передачи и хранения защищаемой информации в электронном виде.	
Машинный носитель персональных данных	Машинный носитель информации, на которых хранятся и (или) обрабатываются персональные данные	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.4. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСБ России 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 требованиям к защите персональных данных для каждого из уровней защищенности»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.5. Пользователи информационных систем должны быть ознакомлены с настоящей Инструкцией до начала работы в информационных системах. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Обязанности пользователей информационных систем

2.1. Пользователи информационных систем обязаны знать и выполнять требования законодательства Российской Федерации и локальных актов Учреждения, устанавливающих правила обработки и защиты ПДн в информационных системах.

2.2. При эксплуатации информационных систем с целью защиты ПДн пользователь обязан:

- руководствоваться требованиями организационно–распорядительной документации по организации обработки и защиты персональных данных;
- соблюдать установленную технологию обработки и защиты ПДн;
- знать свои идентификаторы и пароли, осуществлять ввод паролей в условиях, исключающих их просмотр;
- не записывать значения паролей на бумагу, электронные носители, иные предметы и не разглашать (не сообщать или любым другим способом не доводить

до кого либо, включая работников Учреждения, в т.ч. руководителей, администратора безопасности и системного администратора) значения действующих паролей;
- осуществлять смену пароля не реже, чем через 90 дней;
- надежно хранить индивидуальный аппаратный аутентификатор, не передавать индивидуальный аппаратный аутентификатор другим лицам;
- ежедневно вести антивирусный контроль на непосредственных средствах вычислительной техники (далее – СВТ);
- проверять вложения электронной почты, съемные машинные носители информации перед началом работы на предмет наличия вредоносного программного обеспечения;
- использовать для записи ПДн только съемные машинные носители информации, учтенные в установленном порядке;
- хранить съемные машинные носители персональных данных в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним;
- использовать для вывода на печать документов, содержащих информацию, находящуюся в информационных системах, только устройства печати, расположенные в пределах установленных контролируемых зон, сводя к минимуму возможность доступа к ним посторонних лиц.

2.3. Пользователь должен свести к минимуму возможность неконтролируемого доступа к средствам вычислительной техники информационных систем посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на СВТ работ.

В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются СВТ информационных систем, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить СВТ.

Защищаемые носители информации должны быть убраны в запираемые хранилища, определенные в установленном порядке для этих целей.

2.4. Докладывать администратору безопасности и своему непосредственному руководителю (при наличии):
- о фактах имевшегося или предполагаемого несанкционированного доступа к информации, носителям информации, СВТ информационных систем, помещениям, в которых располагаются СВТ информационных систем, и хранилищам;
- об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка ПДн и хранилищ;
- об обнаружении вредоносного ПО (сообщение на экране монитора о наличии вируса), при иных предупреждающих сообщений средств антивирусной защиты (истечения срока лицензии, о неактуальности базы данных признаков вредоносных компьютерных программ (вирусов) и т.п.), а также при нетипичном поведении СВТ информационных систем (медленная работа при открытии приложений, частое зависание ПО, самопроизвольный перезапуск, сбои в работе);
- о попытках получения информации лицами, не имеющими к ней допуска;
- о попытках неконтролируемого проникновения посторонних лиц в помещения контролируемой зоны информационных систем;

- об иных внештатных ситуациях, связанных с угрозой безопасности информационных систем.

2.5. Пользователю запрещается:

- подключать к СВТ информационных систем нештатные устройства;
- применять в информационных системах незарегистрированные машинные носители информации либо использовать учтенные машинные носители информации в неслужебных целях;
- выносить машинные носители информации, мобильные технические средства данных за пределы контролируемой зоны Учреждения без письменного разрешения руководителя;
- несанкционированно вносить незарегистрированные машинные носители информации, мобильные технические средства;
- блокировать, изменять настройки и выгружать антивирусное ПО на своих СВТ;
- самостоятельно осуществлять подключение (отключение) СВТ к локальной вычислительной сети;
- продолжать работы на СВТ при обнаружении вредоносного ПО в процессе обработки информации;
- самостоятельно вносить изменения в состав, конфигурацию и размещение СВТ информационных систем;
- самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в информационных системах;
- самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (далее – СЗИ) информационных систем;
- сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от хранилищ и помещений и другие реквизиты доступа к информационным системам;
- разрешать работу с СВТ информационных систем лицам, не допущенным к обработке ПДн в установленном порядке;
- находиться в нерабочее время в помещениях, где размещено оборудование информационных систем и СЗИ без служебной записки (или иного вида разрешающего документа), подписанного руководителем Учреждения.

3. Права пользователей информационных систем

3.1. Пользователь информационных систем имеет право:

- обращаться к администратору безопасности, системному администратору информационных систем и ответственному за организацию обработки ПДн по любым вопросам, касающихся обработки и защиты информации в информационных системах (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации информационных систем);
- обращаться к администратору безопасности с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в информационных системах информации, а также по вопросам эксплуатации установленных средств защиты информации (СЗИ);
- обращаться к администратору безопасности с просьбой об оказании консультаций и технической помощи по использованию установленных программных и технических средств информационных систем.

4. Ответственность

4.1. На пользователя информационных систем возлагается персональная ответственность:

- за соблюдение установленной технологии обработки ПДн;
- за соблюдение режима конфиденциальности информации;
- за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в информационных системах;
- за соблюдение требований локальных актов по вопросам обработки и защиты ПДн в информационных системах.

4.2. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 11

УТВЕРЖДЕН
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Порядок доступа в помещения, в которых размещены информационные системы персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»

1. Общие положения

1.1. Настоящий Порядок доступа в помещения, в которых размещены информационные системы персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее - Порядок) определяет в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) порядок организации режима безопасности помещений, в которых размещены информационные системы персональных данных (далее – информационные системы), правила доступа в помещения, в которых размещены информационные системы, в рабочее, нерабочее время и в нештатных ситуациях.

1.2. Сокращения, термины и определения:

В настоящем Порядке используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ПДн	Персональные данные
Помещения	Помещения, в которых размещены информационные системы (технические средства информационных систем, включая средства защиты информации)

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Контролируемая зона	Пространство, в пределах которого	ГОСТ Р 56115-

Термин	Определение	Источник
	осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств	2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработан Порядок:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Пользователи информационных систем должны быть ознакомлены с настоящим Порядком до начала работы в информационных системах под подпись.

1.5. Обязанность по организации ознакомления пользователей с настоящей Порядком возлагается на ответственного за организацию обработки ПДн в Учреждении.

2. Порядок организации режима обеспечения безопасности Помещений.

2.1. Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки персональных данных, средств защиты информации и носителей персональных данных, а также исключается возможность неконтролируемого проникновения и пребывания в этих Помещениях посторонних лиц.

2.2. Перечень Помещений в Учреждении определяется распорядительным актом Учреждения.

2.3. Помещения оснащаются входными дверями с замками, оборудованными механическими замками.

2.4. Вскрытие и закрытие Помещений производится работниками Учреждения, имеющих право доступа в данные Помещения.

2.5. Ключи от Помещений хранятся у работников Учреждения либо в ином порядке, устанавливаемом Инструкцией по обеспечению внутриобъектового и пропускного режима в Учреждении, утверждаемого распорядительным актом Учреждения.

2.6. Организация режима обеспечения безопасности Помещений, где размещены используемые криптосредства, хранятся и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств осуществляется в соответствии с Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в Учреждении.

2.7. Внутренний контроль за соблюдением порядка доступа в Помещения осуществляется ответственным за организацию обработки ПДн.

3. Правила доступа в контролируемую зону в рабочее, нерабочее время, в нештатных ситуациях

3.1. На период обработки защищаемых ПДн в помещениях, где размещено оборудование информационных систем и средств защиты информации, могут находиться только работники, допущенные к обработке персональных данных в соответствии с утвержденным распорядительным актом Учреждения Перечнем лиц, имеющих право доступа в помещения, в которых размещены информационные системы.

3.2. В нерабочее время пребывание вышеуказанных работников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных руководителем Учреждения.

3.3. Нахождение в помещениях контролируемых зон информационных систем других лиц (например, для проведения необходимых профилактических или ремонтных работ, посетителей) возможно только в присутствии работника, допущенного к обработке персональных данных в настоящем помещении.

3.4. Запрещается бесконтрольное нахождение в помещениях контролируемой зоны посторонних лиц в рабочее и нерабочее время.

3.5. Руководитель Учреждения и лица, его замещающие, могут находиться в помещениях контролируемой зоны в любое время, в том числе в нерабочие и праздничные дни.

3.6. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать непосредственно руководителю Учреждения.

3.7. Сотрудники территориальных подразделений Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и аварийных служб, врачи «скорой медицинской помощи» допускаются в помещения контролируемой зоны информационных систем для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя Учреждения.

4. Ответственность

4.1. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в соответствии с действующим законодательством Российской Федерации.

Приложение № 11

УТВЕРЖДЕН
распоряжением
МУ «ВРМЦ»

от 21 апреля 2025 года № 234

Порядок **доступа в помещения, в которых размещены информационные системы персональных данных в Муниципальном учреждении «Всеволожский районный методический центр»**

1. Общие положения

1.1. Настоящий Порядок доступа в помещения, в которых размещены информационные системы персональных данных в Муниципальном учреждении «Всеволожский районный методический центр» (далее - Порядок) определяет в Муниципальном учреждении «Всеволожский районный методический центр» (далее – Учреждение) порядок организации режима безопасности помещений, в которых размещены информационные системы персональных данных (далее – информационные системы), правила доступа в помещения, в которых размещены информационные системы, в рабочее, нерабочее время и в нештатных ситуациях.

1.2. Сокращения, термины и определения:

В настоящем Порядке используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ПДн	Персональные данные
Помещения	Помещения, в которых размещены информационные системы (технические средства информационных систем, включая средства защиты информации)

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Контролируемая зона	Пространство, в пределах которого	ГОСТ Р 56115-

Термин	Определение	Источник
	осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств	2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработан Порядок:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Пользователи информационных систем должны быть ознакомлены с настоящим Порядком до начала работы в информационных системах под подпись.

1.5. Обязанность по организации ознакомления пользователей с настоящей Порядком возлагается на ответственного за организацию обработки ПДн в Учреждении.

2. Порядок организации режима обеспечения безопасности Помещений.

2.1. Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки персональных данных, средств защиты информации и носителей персональных данных, а также исключается возможность неконтролируемого проникновения и пребывания в этих Помещениях посторонних лиц.

2.2. Перечень Помещений в Учреждении определяется распорядительным актом Учреждения.

2.3. Помещения оснащаются входными дверями с замками, оборудованными механическими замками.

2.4. Вскрытие и закрытие Помещений производится работниками Учреждения, имеющих право доступа в данные Помещения.

2.5. Ключи от Помещений хранятся у работников Учреждения либо в ином порядке, устанавливаемом Инструкцией по обеспечению внутриобъектового и пропускного режима в Учреждении, утверждаемого распорядительным актом Учреждения.

2.6. Организация режима обеспечения безопасности Помещений, где размещены используемые криптосредства, хранятся и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств осуществляется в соответствии с Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в Учреждении.

2.7. Внутренний контроль за соблюдением порядка доступа в Помещения осуществляется ответственным за организацию обработки ПДн.

3. Правила доступа в контролируемую зону в рабочее, нерабочее время, в нештатных ситуациях

3.1. На период обработки защищаемых ПДн в помещениях, где размещено оборудование информационных систем и средств защиты информации, могут находиться только работники, допущенные к обработке персональных данных в соответствии с утвержденным распорядительным актом Учреждения Перечнем лиц, имеющих право доступа в помещения, в которых размещены информационные системы.

3.2. В нерабочее время пребывание вышеуказанных работников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных руководителем Учреждения.

3.3. Нахождение в помещениях контролируемых зон информационных систем других лиц (например, для проведения необходимых профилактических или ремонтных работ, посетителей) возможно только в присутствии работника, допущенного к обработке персональных данных в настоящем помещении.

3.4. Запрещается бесконтрольное нахождение в помещениях контролируемой зоны посторонних лиц в рабочее и нерабочее время.

3.5. Руководитель Учреждения и лица, его замещающие, могут находиться в помещениях контролируемой зоны в любое время, в том числе в нерабочие и праздничные дни.

3.6. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать непосредственно руководителю Учреждения.

3.7. Сотрудники территориальных подразделений Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и аварийных служб, врачи «скорой медицинской помощи» допускаются в помещения контролируемой зоны информационных систем для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя Учреждения.

4. Ответственность

4.1. Работники Учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в соответствии с действующим законодательством Российской Федерации.