ПРИЛОЖЕНИЕ № 1

к приказу директора ГКУ НСО «РЦМЦСР»

от \_\_\_\_\_\_\_\_\_\_\_ № \_\_\_

**Политика в отношении обработки персональных данных**

**1. Общие положения**

1.1. Настоящая политика в отношении обработки персональных данных (далее - Политика) определяет порядок обработки и защиты персональных данных в государственном казенном учреждении Новосибирской области «Региональный центр мониторинга цен строительных ресурсов» (далее - Оператор, ГКУ НСО «РЦМЦСР»), в том числе:

1) цели и правила обработки персональных данных, содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении законных оснований;

2) правила рассмотрения запросов субъектов персональных данных или их представителей;

3) правила осуществления внутреннего контроля соответствия обработки персональных данных в ГКУ НСО «РЦМЦСР» требованиям к защите персональных данных, установленных Федеральным [законом](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=06.04.2023) от 27.07.2006 N 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) и принятыми в соответствии с ним нормативными правовыми актами Российской Федерации;

4) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в ГКУ НСО «РЦМЦСР»;

5) порядок доступа работников ГКУ НСО «РЦМЦСР» (далее - работники) в помещения, в которых ведется обработка персональных данных.

1.2. Политика действует в отношении всех персональных данных, которые обрабатывает Оператор.

1.3. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных к настоящей Политике обеспечен неограниченный доступ.

1.4. Основные понятия, используемые в Политике:

**персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

**оператор 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;

**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.

**автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

**распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

**предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

**блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

**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;

**обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

**информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5. Основные права и обязанности Оператора.

1.5.1. Операторимеет право:

1. самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;
2. поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом государственного контракта. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;
3. в случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных.

1.5.2. Операторобязан:

1. организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;
2. отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;
3. сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) по запросу этого органа необходимую информацию в течение 10 рабочих дней с даты получения такого запроса. Данный срок может быть продлен, но не более чем на 5 рабочих дней. Для этого Оператору необходимо направить в Роскомнадзор мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации;
4. в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, которые повлекли неправомерную передачу (предоставление, распространение, доступ) персональных данных.

1.6. Основные права субъекта персональных данных.

1.6.1. Субъект персональных данных имеет право:

1. получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;
2. требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
3. обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

1.7. Трансграничная передача персональных данных на территорию иностранных государств Оператором не осуществляется.

1.8. Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, ответственным за организацию обработки персональных данных.

Уполномоченное лицо, ответственное за организацию обработки персональных данных, непосредственно осуществляющее обработку персональных данных, в случае расторжения с ним трудового договора, обязано прекратить обработку персональных данных, ставших известными ему в связи с исполнением своих обязанностей. Форма такого обязательства утверждается приказом директора ГКУ НСО «РЦМЦСР».

1.9. Ответственность за нарушение требований законодательства Российской Федерации и нормативных актов ГКУ НСО «РЦМЦСР» в сфере обработки и защиты персональных данных определяется в соответствии с законодательством Российской Федерации.

**2. Цели сбора персональных данных**

2.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.3. Обработка Оператором персональных данных осуществляется в следующих целях:

* осуществление своей деятельности в соответствии с уставом ГКУ НСО «РЦМЦСР»;
* исполнение трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, в том числе: содействие работникам в трудоустройстве, получении образования и продвижении по службе, привлечение и отбор кандидатов на работу у Оператора, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, ведение кадрового, бухгалтерского и воинского учета, заполнение и передача в уполномоченные органы требуемых форм отчетности, организация постановки на индивидуальный (персонифицированный) учет работников в системах обязательного пенсионного страхования и обязательного социального страхования, осуществление расчета заработной платы и иных выплат и удержаний.

2.4. Обработка персональных данных работников может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

**3. Правовые основания обработки персональных данных**

3.1. Правовым основанием обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, в том числе:

* Конституция Российской Федерации;
* Гражданский кодекс Российской Федерации;
* Трудовой кодекс Российской Федерации;
* Налоговый кодекс Российской Федерации;
* Федеральный закон от 12.01.1996 № 7-ФЗ «О некоммерческих организациях»;
* Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
* Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
* Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
* Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
* Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;
* Федеральный закон [от 31.05.1996](https://normativ.kontur.ru/document?moduleId=1&documentId=282926) № 61-ФЗ «Об обороне»;
* Федеральный закон от 26.02.1997 № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации»;
* Федеральный закон от 02.05.2006 N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
* Постановление Правительства РФ от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»;
* Приказ Минтруда России от 19.05.2021 N 320н «Об утверждении формы, порядка ведения и хранения трудовых книжек»;
* «Методические рекомендации по ведению воинского учета в организациях» (утв. Генштабом Вооруженных Сил РФ 11.07.2017);
* иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора.

3.2. Правовым основанием обработки персональных данных также являются:

* устав ГКУ НСО «РЦМЦСР»;
* договоры, заключаемые между Оператором и субъектами персональных данных;
* согласия субъектов персональных данных на обработку их персональных данных.

**4. Объем и категории обрабатываемых персональных данных,**

**категории субъектов персональных данных**

4.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разд. 2 настоящей Политики. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. Оператор может обрабатывать персональные данные следующих категорий субъектов персональных данных.

4.2.1. Кандидаты для приема на работу к Оператору - для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений:

* фамилия, имя, отчество;
* пол;
* гражданство;
* дата и место рождения;
* номер контактного телефона и/или сведения о других способах связи;
* сведения об образовании, опыте работы, квалификации;
* иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

4.2.2. Работники и бывшие работники Оператора - для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений:

* фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
* пол;
* гражданство;
* дата и место рождения;
* изображение (фотография);
* паспортные данные;
* адрес регистрации по месту жительства;
* адрес фактического проживания;
* номер контактного телефона и/или сведения о других способах связи;
* индивидуальный номер налогоплательщика;
* страховой номер индивидуального лицевого счета (СНИЛС);
* сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
* семейное положение, наличие детей, родственные связи, сведения и документы, подтверждающие указанные данные;
* личные дела, трудовые книжки и сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий;
* данные о регистрации и/или расторжении брака;
* содержание трудового договора;
* содержание декларации, подаваемой в налоговую инспекцию;
* подлинники и копии приказов по личному составу;
* сведения о трудовом и общем стаже;
* сведения о предыдущем месте работы;
* основания к приказам по личному составу;
* дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
* копии отчетов, направляемые в органы статистики;
* копии документов об образовании;
* результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
* сведения о воинском учете;
* сведения об инвалидности;
* сведения об удержании алиментов;
* сведения о доходе с предыдущего места работы;
* сведения о заработной плате работника;
* сведения о социальных льготах;
* профессия, специальность;
* занимаемая должность;
* размер заработной платы;
* наличие судимостей;
* рекомендации, характеристики;
* принадлежность лица к конкретной нации, этнической группе, расе;
* информация о владении иностранными языками и языками народов Российской Федерации;
* привычки и увлечения, в том числе вредные (алкоголь, наркотики и др.);
* религиозные и политические убеждения (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе, и др.);
* финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);
* сведения о расчетных банковских счетах для перечисления заработной платы и других выплат, связанных с трудоустройством
* деловые и иные личные качества, которые носят оценочный характер;
* прочие сведения, которые могут идентифицировать человека.

Из указанного списка Оператор вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

4.2.3. Члены семей работников Оператора - для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений:

* фамилия, имя, отчество;
* степень родства;
* год рождения;
* иные персональные данные, предоставляемые работниками в соответствии с требованиями действующего законодательства.

4.2.4. Физические лица, обращающиеся в адрес Оператора, за получением государственных услуг, которые могут оказываться Оператором или для реализации права на обращение в соответствии с нормами Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» - для целей осуществления своей деятельности в соответствии с уставом ГКУ НСО «РЦМЦСР»:

* фамилия, имя, отчество;
* адрес регистрации по месту жительства;
* номер контактного телефона и/или сведения о других способах связи;
* иные персональные данные, предоставляемые физическими лицами для получения государственных услуг.

4.3. Оператором не осуществляется обработка биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

4.4. Оператором не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

**5. Порядок и условия обработки персональных данных**

5.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

5.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

5.3. Оператор осуществляет обработку персональных данных для каждой цели их обработки следующими способами:

* неавтоматизированная обработка персональных данных;
* автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
* смешанная обработка персональных данных.

5.4. К обработке персональных данных допускаются работники Оператора, определённые в качестве уполномоченных лиц, ответственных за организацию обработки персональных данных.

5.5. Обработка персональных данных для каждой цели обработки, указанной в п. 2.3 Политики, осуществляется путем:

* получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;
* внесения персональных данных в журналы, реестры и информационные системы Оператора;
* использования иных способов обработки персональных данных.

5.6. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 № 18.

5.7. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Социальный фонд России и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

5.8. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и других несанкционированных действий, в том числе:

* назначает лицо, ответственное организацию обработки персональных данных;
* издает документы, определяющие политику Оператора в отношении обработки персональных данных, локальные нормативные акты и иные документы, в соответствии с требованиями Закона о персональных данных;
* осуществляет внутренний контроль соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам Оператора;
* оценивает вред, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, соотносит указанный вред и принимаемые Оператором меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;
* осуществляет ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и (или) организует их обучение;
* определяет угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;
* применяет организационные и технических меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
* с учетом возможного вреда субъекта персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных определяет уровни защищенности персональных данных при их обработке в информационных системах персональных данных;
* применяет прошедшие в установленном порядке процедуру оценки соответствия средств защиты информации;
* осуществляет оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
* осуществляет учет машинных носителей персональных данных;
* обнаруживает факты несанкционированного доступа к персональным данным и принимает меры, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
* восстанавливает персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
* устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;
* обеспечивает доступ к информационным системам персональных данных осуществляется с использованием уникального пароля и (или) с помощью электронно-цифровой подписи;
* создает необходимые условия для работы с персональными данными;
* организует учет документов, информационных систем и электронных носителей (при наличии), а также архивных копий (при наличии), содержащих персональные данные;
* организует работу с информационными системами, в которых обрабатываются персональные данные;
* хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним, в том числе организует режим обеспечения безопасности помещений, в которых размещена информационная система, а также находятся персональные данные, обработка которых осуществляется без использования средств автоматизации, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
* утверждает [перечень](https://internet.garant.ru/#/document/70742338/entry/1000) лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей;
* обеспечивает раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях без использования средств автоматизации;
* обеспечивает антивирусную защиту информационной системы;
* устанавливается уровень защищенности персональных данных при их обработке в информационной системе персональных данных;
* осуществляет контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных;
* принимает иные меры по обеспечению безопасности персональных данных при их обработке, установленные законодательством.

5.9. Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требует каждая цель обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

5.9.1. Персональные данные на бумажных носителях хранятся в ГКУ НСО «РЦМЦСР» в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 N 125-ФЗ «Об архивном деле в Российской Федерации», Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 N 236)).

5.9.2. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

5.10. Оператор прекращает обработку персональных данных в следующих случаях:

* выявлен факт их неправомерной обработки. Срок - в течение 3 рабочих дней с даты выявления;
* достигнута цель их обработки;
* истек срок действия или отозвано согласие субъекта персональных данных на обработку указанных данных, когда по Закону о персональных данных обработка этих данных допускается только с согласия.

5.11. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку Оператор прекращает обработку этих данных, если:

* иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
* Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;
* иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

5.12. При обращении субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных в срок, не превышающий 10 рабочих дней с даты получения Оператором соответствующего требования, обработка персональных данных прекращается, за исключением случаев, предусмотренных Законом о персональных данных. Указанный срок может быть продлен, но не более чем на 5 рабочих дней. Для этого Оператору необходимо направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока.

5.13. При сборе персональных данных Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

5.14. В целях информационного обеспечения Оператор может создавать общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

**6. Актуализация, исправление, удаление, уничтожение персональных**

**данных, ответы на запросы субъектов на доступ к персональным данным**

6.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Оператором субъекту персональных данных или его представителю в течение 10 рабочих дней с момента обращения либо получения запроса субъекта персональных данных или его представителя. Данный срок может быть продлен, но не более чем на 5 рабочих дней. Для этого Оператору следует направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.

В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

Запрос должен содержать:

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

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

Оператор предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение 7 рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.3. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

6.4. При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор:

* в течение 24 часов - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;
* в течение 72 часов - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

6.5. Порядок уничтожения персональных данных Оператором.

6.5.1. Условия и сроки уничтожения персональных данных Оператором:

* достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - в течение 30 дней;
* достижение максимальных сроков хранения документов, содержащих персональные данные, - в течение 30 дней;
* предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, - в течение 7 рабочих дней;
* невозможность обеспечения правомерности обработки персональных данных, - в течение 10 рабочих дней с даты выявления неправомерной обработки персональных данных.
* отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

6.5.2. При достижении целей обработки персональных данных, или в случае утраты необходимости в достижении этих целей, а также в случае отзыва субъектом персональных данных согласия на их обработку, или в случае, если обеспечить правомерность обработки персональных данных невозможно, персональные данные подлежат уничтожению, если:

* иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
* оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;
* иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

6.5.3. Уничтожение персональных данных осуществляется комиссией, состав и порядок работы, которой утверждается приказом директора ГКУ НСО «РЦМЦСР».

6.5.4. При уничтожении персональных данных необходимо:

* убедиться в необходимости уничтожения персональных данных;
* убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;
* уничтожить персональные данные подходящим способом в соответствии с настоящей Политикой или способом, указанным в соответствующем требовании или распорядительном документе;
* проверить необходимость уведомления об уничтожении персональных данных;
* при необходимости уведомить об уничтожении персональных данных требуемых лиц.

При уничтожении персональных данных применяются следующие способы:

* сжигание, передача специализированной организации для уничтожения, измельчение, в том числе с помощью применения бумагорезательной (бумагоуничтожительной) машины, – для документов, исполненных на бумаге;
* физическое уничтожение частей носителей информации – разрушение или сильная деформация для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы);
* уничтожение модулей и микросхем долговременной памяти СD (DVD)-дисков, USB- и Flash-носителей;
* стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и в отдельных документах на машинном носителе.

При необходимости уничтожения части персональных данных допускается уничтожать материальный носитель одним из указанных в настоящей Политике способов с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

По факту уничтожения персональных данных составляется акт об уничтожении персональных данных, который подписывается лицами, производившими уничтожение, утверждается председателем комиссии, и производится выгрузка из журнала регистрации событий в информационной системе персональных данных, в случае, когда производилось уничтожение персональных данных, обработка которых осуществлялась Оператором с использованием средств автоматизации.

Требования к акту об уничтожении персональных данных и выгрузке из журнала устанавливаются Приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

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

**7. Внутренний контроль соответствия обработки персональных**

**данных законодательству, требованиям к защите персональных данных**

7.1. Внутренний контроль соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Политике, иным локальным актам Оператора в сфере персональных данных осуществляется путем проведения проверок создаваемой для этих целей комиссией ГКУ НСО «РЦМЦСР».

Состав комиссии утверждается приказом директора ГКУ НСО «РЦМЦСР».

7.2. Проверки проводятся по решению директора ГКУ НСО «РЦМЦСР» не реже одного раза в три года.

Решение о проведении внеплановой проверки может быть принято в следующих случаях:

* в случае поступления письменного заявления владельца персональных данных или его представителя о нарушениях правил обработки персональных данных;
* по результатам расследования инцидента информационной безопасности;
* по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных.

При наступлении любого из вышеуказанных случаев проверки назначаются не позднее рабочего дня, следующего за днем наступления такого случая.

Проверка должна быть завершена не позднее чем через 30 календарных дней со дня принятия решения о ее проведении. При наличии оснований срок проведения проверки может быть продлен на 30 календарных дней.

7.3. По результатам проверки составляется акт. Акт подписывается всеми лицами, входящими в состав комиссии.

7.4. В случае выявления нарушений условий обработки персональных данных в акте указываются причины нарушения, лица, виновные в возникновении нарушения, и перечень мер, необходимых для устранения нарушения, в случае невозможности их устранения в ходе проверки.

7.5. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

* полнота и качество выполнения организационных и технических мер по обеспечению безопасности персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
* порядок и условия применения средств защиты информации;
* состояние учета машинных носителей персональных данных;
* соблюдение правил доступа к персональным данным;
* наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
* своевременность и полнота принятых мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
* полнота и качество принимаемых мер по обеспечению целостности персональных данных.

7.6. Комиссия имеет право:

* запрашивать у работников ГКУ НСО «РЦМЦСР» информацию, необходимую для проведения проверки;
* принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
* вносить директору ГКУ НСО «РЦМЦСР» предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
* вносить директору ГКУ НСО «РЦМЦСР» предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации при обработке персональных данных;
* осуществление иных полномочий, установленных Положением о комиссии.

**8. Процедуры, направленные на выявление и предотвращение**

**нарушений, предусмотренных законодательством в сфере персональных данных**

8.1. К процедурам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, осуществляемых Оператором относятся:

* осуществление внутреннего контроля соответствия обработки персональных данных Оператором требованиям к защите персональных данных, установленных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, Политикой, иными локальными актами Оператора в сфере персональных данных;
* оценка вреда, который может быть причинен владельцам персональных данных в случае нарушения положений Закона о персональных данных и принятых в соответствии с ним нормативных правовых актов, требований к защите персональных данных, а также Политики;
* ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации в сфере персональных данных, в том числе требованиями к защите персональных данных, документами Оператора в отношении обработки персональных данных.

8.2. Обеспечение безопасности персональных данных у Оператора достигается с помощью мер, определенных статьей 19 Закона о персональных данных, в том числе:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в порядке, установленном в соответствии с законодательством Российской Федерации, процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных.

**9. Порядок доступа в помещения,**

**в которых ведется обработка персональных данных**

9.1. Персональные данные относятся к конфиденциальной информации, работники Оператора, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия владельца персональных данных, если иное не предусмотрено федеральными законами.

9.2. В помещениях, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время.

По завершении рабочего дня помещения, в которых ведется обработка персональных данных, закрываются.

Хранение носителей персональных данных осуществляется в условиях, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

9.3. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители персональных данных, допускаются только лица, уполномоченные на обработку персональных данных, а также лица доступ которых к персональным данным, в том числе обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей.

9.4. Нахождение в помещениях Оператора, в которых ведется обработка персональных данных, иных лиц, возможно только в присутствии, лиц, указанных в п 9.3. Политики, на время, ограниченное необходимостью решения вопросов, входящих в должностные обязанности работников Оператора, а также связанных с осуществлением полномочий и функций и (или) выполнением обязательств Оператора в рамках действующего законодательства.

9.5. Ответственность за соблюдение порядка доступа в помещения Оператора, в которых ведется обработка персональных данных, возлагается на ответственного за организацию обработки персональных данных.