

Утверждено
приказом директора
ГБУ «ЦСОГПВИИ г. Арзамаса»
№ 01-16/216 от 08.12.2014 г.



Правила обработки персональных данных в ГБУ «ЦСОГПВИИ г. Арзамаса»

1. Общие положения

1.1. Настоящие «Правила обработки персональных данных в государственном бюджетном учреждении «Центр социального обслуживания граждан пожилого возраста и инвалидов города Арзамаса» (далее — Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных») и другими нормативно-правовыми актами.

1.2. Настоящие Правила определяют основные требования к порядку обработки (как с использованием средств автоматизации, так и без использования таковых) и обеспечения безопасности персональных данных, а также обязанности должностных лиц государственного бюджетного учреждения «Центр социального обслуживания граждан пожилого возраста и инвалидов города Арзамаса» (далее – Учреждение) в процессе обработки персональных данных. Под субъектами персональных данных (далее – Субъект ПДн) понимаются работники (должностные лица) Учреждения, а также иные Субъекты ПДн, в том числе «получатели государственных услуг», «заявители» и т.д.

1.3. Организационно-распорядительные документы Учреждения, касающиеся вопросов обработки персональных данных, необходимо привести в соответствие с настоящими Правилами.

1.4. Требования настоящих Правил являются обязательными для выполнения всеми должностными лицами Учреждения и иными лицами, имеющими договорные отношения с Учреждением.

1.5. Необходимые правовые, организационные и технические меры для защиты персональных данных при их автоматизированной обработке в информационных системах Учреждения и при обработке без использования средств автоматизации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, регламентируются настоящими Правилами.

1.6. В соответствии с требованиями нормативных правовых актов о персональных данных документы, определяющие политику Учреждения в отношении обработки персональных данных и реализуемые общие требования к обработке и защите персональных данных, размещаются на официальном сайте Учреждения.

2. Цели и принципы обработки персональных данных

2.1. Учреждение осуществляет обработку персональных данных в следующих целях:

- а) при осуществлении основной деятельности Учреждения, связанной с необходимостью обработки ПДн, обусловленной требованиями действующего законодательства и нормативно-правовых актов, регламентирующих деятельность Учреждения;
- б) при рассмотрении обращений Субъектов ПДн на предоставление им государственных услуг, включая при необходимости передачу персональных данных третьим лицам;
- в) при прохождении работы, обучении и служебного продвижения должностных лиц Учреждения, формирования кадрового резерва, учета результатов исполнения ими своих

должностных обязанностей, обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций и других целей, связанных с осуществлением трудовых отношений;

г) статистической обработки информации, при условии обязательного обезличивания персональных данных;

д) опубликования информации о деятельности органа власти, согласно требованиям действующего законодательства Российской Федерации.

2.2. Обработка персональных данных в вышеуказанных целях осуществляется в Учреждении на основе следующих принципов:

а) обработка персональных данных должна осуществляться на законной и справедливой основе;

б) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

в) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

г) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

е) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных; оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

ж) хранение персональных данных должно осуществляться в форме, позволяющей определить Субъекта ПДн, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом; обрабатываемые персональные данные подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3. Субъекты персональных данных

3.1. В качестве Субъектов ПДн, персональные данные которых могут обрабатываться в Учреждении с использованием средств автоматизации или без использования таковых, понимаются нижеперечисленные категории физических лиц:

3.2. Лица, в число которых включаются:

3.2.1. Персонал Учреждения, то есть лица, имеющие в настоящее время трудовые отношения, а также ранее имевшие трудовые отношения с Учреждением;

3.2.2. Лица, имеющие договорные отношения гражданско-правового характера с Учреждением;

3.2.3. Лица, проходящие различного рода практику (стажировку) в Учреждении.

3.3. Заявители, в состав которых включаются:

3.3.1. Физические лица и их Представители (лица, действующие по доверенности физических лиц и др.), подающие заявления (обращающиеся) в Учреждение за предоставлением государственных услуг, их поручители, и т.п.;

3.3.2. Руководители, представители и работники юридических лиц (организаций и органов власти), имеющих договорные отношения с Учреждением о межведомственном информационном взаимодействии.

3.3.3. Иные Субъекты ПДн, которые не вошли в вышеперечисленные категории и обработка персональных данных которых не противоречит законодательству РФ.

4. Категории персональных данных.

4.1. В Учреждении в соответствии с Федеральным законом «О персональных данных» выделяются следующие категории персональных данных:

- а) специальные категории персональных данных;
- б) персональные данные общей категории, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным;
- в) обезличенные и/или общедоступные персональные данные.

5. Содержание обрабатываемых персональных данных

5.1. Содержание и объем обрабатываемых персональных данных определяются, исходя из возложенных на Учреждение функций и выполняемых задач, согласно законодательству Российской Федерации и Нижегородской области. В состав персональных данных Субъектов ПДн, обрабатываемых в Учреждении могут входить:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора (гражданско-правового договора);
- сведения о доходах и наличии материальных ценностей;
- личные дела и трудовые книжки работников;
- другие сведения.

5.2. Конкретный состав персональных данных Субъектов ПДн определяется перечнями, утверждаемыми директором Учреждения, для различных целей обработки.

6. Назначение ответственных лиц

6.1. В Учреждении распорядительным документом назначается лицо, ответственное за организацию обработки персональных данных, как с использованием средств автоматизации, так и без использования таковых (далее - ответственный за организацию обработки персональных данных). Ответственный за организацию обработки персональных данных несёт ответственность за указанную деятельность перед директором Учреждения и подотчетен ему.

В соответствии с требованиями Федерального закона «О персональных данных» ответственный за организацию обработки персональных данных, в частности обязан:

- осуществлять внутренний контроль соблюдения Учреждением, как оператором персональных данных, и его должностными лицами законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения должностных лиц Учреждения требования законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов Субъектов ПДн или их представителей и осуществлять контроль приема и обработки таких обращений и запросов. На время отсутствия ответственного за организацию обработки персональных данных его обязанности исполняет должностное лицо, его замещающее.

6.2. На ответственного за организацию обработки персональных данных возлагается задача по организации выполнения законодательных требований при обработке персональных данных в Учреждении.

6.3. Ответственными за организацию выполнения требований внутренних организационно-распорядительных документов Учреждения по вопросам обработки персональных данных и их защите в структурных подразделениях Учреждения являются руководители этих подразделений. На время отсутствия этих руководителей ответственными являются лица, замещающие их по штатному расписанию.

6.4. Ответственными за выполнение требований организационно-распорядительных документов Учреждения по вопросам обработки персональных данных и их защите непосредственно на своих рабочих местах в рамках определенных соответствующими должностными инструкциями являются лица, уполномоченные в установленном порядке обрабатывать в Учреждении персональные данные.

7. Должностные лица, уполномоченные обрабатывать персональные данные

7.1. Должностные лица, уполномоченные обрабатывать в Учреждении персональные данные, как с использованием средств автоматизации, так и без использования таковых, подразделяются на следующие группы:

- а) обрабатывающие персональные данные только работников Учреждения;
- б) обрабатывающие персональные данные только заявителей (представителей юридических лиц), обращающихся в Учреждение, в том числе и за оказанием государственных услуг. Должностные лица, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены с требованиями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, организационно-распорядительными документами Учреждения, определяющими политику в отношении обработки персональных данных.

8. Сроки обработки и хранения обрабатываемых персональных данных

8.1. Сроки обработки персональных данных должны ограничиваться достижением конкретных, заранее определенных и законных целей.

8.2. Процедура хранения персональных данных в Учреждении проводится в порядке, который позволяет осуществлять хранение персональных данных в форме, позволяющей определить Субъекта ПДн, не дольше, чем этого требуют цели обработки персональных данных, если срок их хранения не установлен федеральным законом.

8.3. Сроки хранения персональных данных в Учреждении, в общем случае, определяются в соответствие со сроками, установленными требованиями законодательства РФ, нормативных документов федеральных органов исполнительной власти.

8.4. Сроки хранения персональных данных указываются в документах, подтверждающих получение согласия Субъекта ПДн на обработку его персональных данных или во внутренних организационно-распорядительных документах Учреждения.

9. Допуск к обработке персональных данных

9.1. Для должностных лиц, обрабатывающих персональные данные как с использованием средств автоматизации, так и без использования таковых, в соответствии со своими должностными обязанностями и (или) в рамках договорных отношений, допуск производится в соответствии с перечнем должностных лиц, допущенных к обработке персональных данных.

9.2. Для исключения преднамеренного или непреднамеренного доступа посторонних лиц к персональным данным и носителям, их содержащим, при необходимости может быть введен пропускной режим в здание (помещение) Учреждения и определен порядок приема, учета и контроля деятельности посетителей.

10. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

10.1. С целью предотвращения нарушений законодательства Российской Федерации в сфере персональных данных ответственный за обработку персональных данных обязан организовать и провести следующие процедуры (мероприятия, работы):

10.1.1. Направление уведомления об обработке персональных данных в контролирующий орган (Роскомнадзор);

10.1.2. Разработку формы согласия Субъекта ПДн на обработку его персональных данных (согласие должно содержать собственноручную подпись Субъекта ПДн (либо его цифровую подпись);

10.1.3. Документальное описание информационных систем обработки персональных данных (назначение, состав, категории ПДн, правовые основания для их обработки), а также перечень должностных лиц, работающих с персональными данными и имеющими к ним доступ, с разграничением прав доступа к ПДн;

10.1.4. Разработку организационно-распорядительных документов, описывающих угрозы ПДн и мер по их предотвращению с учётом класса ИСПДн;

10.1.5. Обеспечение защиты персональных данных техническими (программными, аппаратными) и организационными методами, независимо от характера обработки ПДн от всех видов утраты (утечки), в том числе от несанкционированного доступа, изменения, разглашения или уничтожения данных, в том числе непреднамеренных;

10.1.6. Обеспечение физической защиты информационных ресурсов (система контроля доступа в здание (помещения), где происходит обработка и хранение ПДн).

10.1.7. Обеспечение квалифицированного информирования (обучения, подготовки, повышения квалификации) исполнителей, ответственных за обработку ПДн.

10.2. С целью выявления возможных нарушений законодательства Российской Федерации в сфере персональных данных при обработке ПДн в Учреждении осуществляется контроль соответствия реального состояния работ с персональными данными требованиям нормативных актов. Мероприятия по внутреннему контролю в Учреждении организуются должностным лицом, ответственным за организацию обработки ПДн.

10.3. Предметом плановых (внеплановых) внутренних проверок состояния работ по обработке ПДн являются:

10.3.1. Наличие и содержание (полнота сведений) уведомления об обработке персональных данных;

10.3.2. Соответствие обработки персональных данных заявленным целям;

10.3.3. Соблюдение требований по уничтожению ПДн после достижения цели их обработки;

10.3.4. Соответствие установленного законом порядка сбора, хранения, использования или распространения информации о гражданах в части обработки персональных данных без согласия Субъекта ПДн;

10.3.5. Соответствие типовых форм документов, содержащих персональные данные, требованиям законодательства;

10.3.6. Наличие перечня должностных лиц, осуществляющих обработку персональных данных с использованием средств автоматизации и без таковых, либо имеющих к ним доступ.

10.3.7. Обеспечение безопасного хранения персональных данных (их материальных носителей).

10.3.8. Прочие аспекты обеспечения безопасности персональных данных в Учреждении.

10.4. Кроме внутреннего контроля, соблюдение требований законодательства Российской Федерации в сфере персональных данных, функции государственного надзора в данной сфере возложен на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (раздел 13 настоящих Правил).

11. Взаимодействие Учреждения с Субъектами ПДн при обработке ПДн

11.1. Согласие Субъекта ПДн.

11.1.1. Согласие на обработку персональных данных может быть дано Субъектом ПДн или его Представителем в любой форме, позволяющей подтвердить факт его получения, если иное не установлено федеральным законом.

11.1.2. Обработка персональных данных допускается в следующих случаях:

- а) обработка персональных данных осуществляется с согласия Субъекта ПДн на обработку его персональных данных;
- б) обработка персональных данных необходима для достижения целей, предусмотренных законодательством Российской Федерации, для осуществления и выполнения возложенных на Учреждение, как на оператора, функций, полномочий и обязанностей;
- в) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- г) обработка персональных данных необходима для предоставления государственной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации Субъекта ПДн на едином портале государственных и муниципальных услуг.
- д) обработка персональных данных необходима для исполнения договора, стороной которого является Субъект ПДн;
- е) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта ПДн, если получение согласия Субъекта ПДн невозможно;
- з) обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;
- и) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен Субъектом ПДн, либо по его просьбе;
- к) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

В случаях, предусмотренных действующим законодательством Российской Федерации, обработка персональных данных осуществляется только с согласия в письменной форме Субъекта ПДн. Равнозначным содержащему собственноручную подпись Субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с действующим законодательством Российской Федерации электронной подписью.

11.1.3. Согласие Субъекта ПДн в письменной форме на обработку его персональных данных должно включать в себя, в частности:

- а) фамилию, имя, отчество, адрес Субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- б) фамилию, имя, отчество, адрес Представителя Субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты Документа, подтверждающего полномочия этого Представителя (при получении согласия от Представителя Субъекта ПДн);
- в) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие Субъекта ПДн;
- г) цель обработки персональных данных;
- д) перечень персональных данных, на обработку которых дается согласие Субъекта ПДн;

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

ж) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

з) срок, в течение которого действует Согласие, а также способ его отзыва, если иное не установлено федеральным законом;

и) подпись Субъекта ПДн.

11.1.4. Согласие Субъекта ПДн или его Представителя в ряде необходимых случаев может быть оформлено отдельным документом.

11.1.5. Субъект ПДн вправе отозвать свое Согласие. В случае отзыва Субъектом ПДн своего Согласия ему необходимо оформить письменный запрос на отзыв с обязательным указанием фамилии, имени, отчества, адреса, номера основного документа, удостоверяющего его личность, сведений о дате выдачи указанного документа и выдавшем его органе, подписать его и передать лично или через своего Представителя. Если Отзыв передается через Представителя, то он должен предъявить документ, подтверждающий полномочия этого Представителя на право представления соответствующих интересов Субъекта ПДн.

11.2. Доступ Субъектов ПДн к обрабатываемым персональным данным

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

а) подтверждение факта обработки персональных данных в Учреждении;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые Учреждением способы обработки персональных данных;

г) наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным;

д) обрабатываемые персональные данные, относящиеся к соответствующему Субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

ж) порядок осуществления Субъектом ПДн прав, предусмотренных Федеральным законом «О персональных данных»;

з) информацию об осуществленной или предполагаемой трансграничной передаче данных;

и) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу. Учреждение обязано сообщить Субъекту ПДн или его Представителю информацию о наличии персональных данных, относящихся к соответствующему Субъекту ПДн, а также предоставить возможность ознакомления с этими персональными данными при обращении Субъекта ПДн или его Представителя либо в течение тридцати дней с даты получения запроса Субъекта ПДн или его Представителя.

11.2.2. Право Субъекта ПДн на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

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

б) обработка персональных данных осуществляется органами, осуществившими задержание Субъекта ПДн по подозрению в совершении преступления, либо предъявившими Субъекту ПДн обвинение по уголовному делу, либо применившими к Субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, если

допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

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

г) доступ Субъекта ПДн к его персональным данным нарушает права и законные интересы третьих лиц;

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

11.2.3. Выбор формы запроса для реализации своего права на получение сведений зависит от воли Субъекта ПДн. Сведения могут быть предоставлены Субъекту ПДн или его Представителю для ознакомления в случае:

а) устного обращения в Учреждение, сопровождающиеся обязательным предоставлением основного документа, удостоверяющего личность Субъекта ПДн или его Представителя, а также Документа, подтверждающего полномочия этого Представителя;

б) предоставления запроса в Учреждение, который может быть исполнен как на бумажном носителе (при личном обращении Субъекта ПДн или его Представителя), так и в форме электронного документа, подписанного электронной подписью в соответствии с законодательством РФ. Запрос должен содержать: данные основного документа, удостоверяющего личность Субъекта ПДн или его Представителя, либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждения, подпись Субъекта ПДн или его Представителя.

11.3. Отказ в предоставлении персональных данных

11.3.1. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем Субъекте ПДн или персональных данных Субъекту ПДн или его Представителю при их обращении либо при получении запроса Субъекта ПДн или его Представителя, орган власти обязан дать в письменной форме мотивированный ответ в срок, не превышающий 30 дней со дня обращения Субъекта ПДн или его Представителя либо с даты получения запроса Субъекта ПДн или его Представителя.

11.4. Прекращение обработки, уточнение, блокирование и уничтожение персональных данных

11.4.1. В случае выявления неправомерной обработки персональных данных при обращении Субъекта ПДн или его Представителя либо по запросу Субъекта ПДн или его Представителя либо уполномоченного органа по защите прав Субъектов ПДн Учреждение обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому Субъекту ПДн, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки.

Решение о блокировании персональных данных соответствующего Субъекта ПДн принимает ответственный за организацию обработки персональных данных.

11.4.2. В случае выявления неточных (неполных, устаревших) персональных данных при обращении Субъекта ПДн или его Представителя либо по их запросу или по запросу уполномоченного органа по защите прав Субъектов ПДн орган власти обязан осуществить блокирование персональных данных, относящихся к этому Субъекту ПДн, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению органа власти) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы Субъектов ПДн или третьих лиц. Решение о блокировании предположительно неточных персональных данных соответствующего

Субъекта ПДн принимает ответственный за организацию обработки персональных данных.

11.4.3. В случае достижения цели обработки персональных данных или в случае утраты необходимости в достижении этих целей Учреждение обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить персональные данные (либо провести обезличивание) или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных, если иное не предусмотрено на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

11.4.4. В случае отзыва Субъектом ПДн согласия на обработку его персональных данных Учреждение обязано прекратить их обработку или обеспечить 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, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством.

11.4.5. В случае отсутствия возможности уничтожения персональных данных в течение срока, определённого настоящими Правилами, Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения), и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

11.4.6. Об устранении допущенных нарушений, в результате которых персональные данные были неполными, неточными или неактуальными и подлежали изменению, или об уничтожении персональных данных (в случае неправомерной обработки персональных данных, т. е. когда они являются незаконно полученными или не являются необходимыми для заявленной цели обработки), Учреждение обязано уведомить Субъекта ПДн или его Представителя.

11.4.7. Учреждение также обязано принять разумные меры для уведомления третьих лиц, которым были переданы персональные данные Субъекта ПДн в случае, когда с целью устранения допущенных нарушений было необходимо обеспечить изменение переданных персональных данных ввиду их неполноты, неточности или неактуальности.

12. Уведомление об обработке персональных данных

12.1. Учреждение обязано уведомить уполномоченный орган по защите прав Субъектов ПДн об осуществлении обработки персональных данных, за исключением следующих случаев обработки персональных данных:

- а) обрабатываемых в соответствии с трудовым законодательством;
- б) полученных оператором в связи с заключением договора, стороной которого является Субъект ПДн, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия Субъекта ПДн и используются оператором исключительно для исполнения указанного договора и заключения договоров с Субъектом ПДн;
- в) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут

распространяться или раскрываться третьим лицам без согласия в письменной форме Субъектов ПДн;

г) сделанных Субъектом ПДн общедоступными;

д) включающих в себя только фамилии, имена и отчества Субъектов ПДн;

е) необходимых в целях однократного пропуска Субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях;

ж) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

з) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав Субъектов ПДн;

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

12.2. Уведомление об обработке персональных данных должно быть направлено в виде документа на бумажном носителе или в форме электронного документа и подписываться уполномоченным лицом.

Уведомление должно содержать следующие сведения:

а) наименование, адрес Учреждения;

б) цель обработки персональных данных;

в) категории персональных данных;

г) категории Субъектов, персональные данные которых обрабатываются;

д) правовое основание обработки персональных данных;

е) перечень действий с персональными данными, общее описание используемых Учреждением способов обработки персональных данных;

ж) описание мер по обеспечению безопасности персональных данных при их обработке, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

з) фамилия, имя, отчество лица, ответственного за организацию обработки персональных данных в Учреждении, и номера его контактных телефонов, почтовые адреса и адреса электронной почты;

и) дата начала обработки персональных данных;

к) срок или условие прекращения обработки персональных данных.

Уполномоченный орган по защите прав Субъектов ПДн в течение 30 дней с даты поступления уведомления об обработке персональных данных вносит вышеуказанные сведения, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными и публикуются на официальном сайте уполномоченного органа по защите прав Субъектов ПДн в глобальной сети Интернет.

12.3. При подготовке уведомления (изменений в уведомление) необходимо руководствоваться официальными рекомендациями уполномоченного органа по защите прав Субъектов ПДн по заполнению образца формы уведомления об обработке персональных данных.

В случае предоставления органом власти неполных или недостоверных сведений, указанных в настоящих Правилах, уполномоченный орган по защите прав Субъектов ПДн вправе требовать от Учреждения уточнения предоставленных сведений до их внесения в реестр операторов.

12.4. В случае изменения сведений, указанных в уведомлении, Учреждение обязано уведомить об изменениях уполномоченный орган по защите прав Субъектов ПДн в течение 10 рабочих дней с даты возникновения таких изменений.

12.5. Необходимость внесения изменений в ранее поданное уведомление в уполномоченный орган по защите прав Субъектов ПДн определяет Ответственный за организацию обработки персональных данных.

13. Взаимодействие с третьими лицами при обработке ПДн

13.1. Передача персональных данных третьим лицам должна осуществляться с согласия Субъекта ПДн, если иное не предусмотрено действующим законодательством.

13.2. Учреждение вправе поручить обработку персональных данных другому лицу с согласия Субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (государственного или муниципального контракта), который должен предусматривать:

- а) перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
- б) цели обработки персональных данных;
- в) обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- г) требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом «О персональных данных».

Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». Лицо, осуществляющее обработку персональных данных на основании договора с Учреждением, не обязано получать согласие Субъекта ПДн на обработку его персональных данных.

В случае если Учреждение поручает обработку персональных данных другому лицу, ответственность перед Субъектом ПДн за действия указанного лица несет Учреждение.

Лицо, осуществляющее обработку персональных данных по поручению Учреждения, несет ответственность перед Учреждением.

13.3. В случае, если Учреждение поручает обработку персональных данных другому лицу, Субъект обрабатываемых ПДн вправе иметь доступ к следующей информации:

- а) наименование и адрес третьего лица;
- б) цель обработки персональных данных и ее правовое основание;
- в) предполагаемые пользователи персональных данных;
- г) установленные Федеральным законом «О персональных данных» права Субъекта ПДн;
- д) источник получения персональных данных.

14. Государственный контроль (надзор) соответствия обработки персональных данных требованиям законодательства РФ в области персональных данных

14.1. Уполномоченным органом по защите прав Субъектов ПДн, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, а именно Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор).

14.2. Роскомнадзор имеет право:

- а) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- б) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных оператора персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

в) требовать от органа власти, как оператора персональных данных, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

г) принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований Федерального закона «О персональных данных»;

д) обращаться в суд с исковыми заявлениями в защиту прав Субъектов ПДн, в том числе в защиту прав неопределенного круга лиц, и представлять интересы Субъектов ПДн в суде;

е) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в пункте 7 части 3 статьи 22 Федерального закона «О персональных данных»;

ж) привлекать к административной ответственности лиц, виновных в нарушении Федерального закона «О персональных данных».

14.3. Уполномоченный представитель органа власти должен обеспечить необходимые условия для проведения проверки и обязан по требованию должностных лиц Роскомнадзора или его территориального органа (далее – Роскомнадзор), проводящих проверку, обеспечить доступ в помещения, где осуществляется обработка персональных данных, предоставить необходимую информацию и документацию для достижения целей проверки.

14.4. По результатам проверки должностными лицами Роскомнадзора, проводившими проверку, составляется акт проверки, который оформляется непосредственно после ее завершения.

15. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации

15.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, строится на принципах, изложенных в «Положении об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденном Постановлением Правительства РФ от 15.09.2008 г. № 687.

15.2. При разработке типовых форм, содержащих персональные данные, ответственные за разработку этих форм отделения Учреждения должны учитывать следующие положения:

а) фиксация на одном материальном носителе персональных данных Субъекта, цели обработки которых несовместимы, не допускается (типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых несовместимы);

б) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать следующие сведения — цель обработки персональных данных, имя (наименование) и адрес органа власти, Ф.И.О. и адрес Субъекта ПДн, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки и общее описание используемых Учреждением способов обработки персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из Субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных Субъектов ПДн.

15.3. В случае организации в Учреждении пропускного режима в здание (помещение) в которых размещаются структурные подразделения Учреждения, при ведении журналов

(реестров, книг), содержащих персональные данные, используемые для однократного пропуска Субъекта ПДн, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) ведение такого журнала (реестра, книги) могут осуществляться без использования средств автоматизации,

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого Субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска Субъекта ПДн в здание (помещения), в которых находятся структурные подразделения Учреждения.

15.4. Для решения задачи обеспечения состояния безопасности, связанной с физическим доступом Субъектов ПДн в помещения Учреждения, в которых производится обработка персональных данных, возможно применение системы видеонаблюдения.

15.5. В организационно-распорядительной документации Учреждения должен быть определен порядок не архивного хранения документов (материальных носителей), содержащих персональные данные, который предусматривает раздельное хранение документов по соответствующим категориям персональных данных и по целям их обработки, с назначением мест хранения и ответственных за хранение с соблюдением конфиденциальности персональных данных и исключением несанкционированного доступа к ним, а также определением мер контроля обеспечения безопасности персональных данных при хранении их материальных носителей.

15.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

15.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

15.8. При необходимости уточнение персональных данных 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 персональными данными.

16. Особенности обработки персональных данных, осуществляемой с использованием средств автоматизации

16.1. Обеспечение безопасности персональных данных при их обработке с использованием средств автоматизации должно производиться в соответствии с

Требованием к защите персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 и иными нормативными актами.

16.2. Автоматизированные технологические процессы, в рамках которых обрабатываются персональные данные в информационных системах Учреждения, должны быть документированы.

16.3. Для каждой ИСПД должны быть определены и зафиксированы:

- а) цель обработки персональных данных;
- б) объем и содержание (категории) обрабатываемых персональных данных;
- в) перечень действий с персональными данными и способы их обработки.

Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. В том случае, если для выполнения технологического процесса, реализацию которого поддерживает ИСПД, нет необходимости в обработке определенных персональных данных, эти персональные данные должны быть удалены.

16.4. В ИСПДн Учреждения наряду с необходимостью обеспечения конфиденциальности персональных данных требуется обеспечить следующие характеристики безопасности персональных данных: защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий.

16.5. В целях обеспечения безопасности персональных данных при их обработке в ИСПДн, на основе оценки рисков нарушения безопасности персональных данных, в Учреждении разрабатывается частная модель угроз безопасности персональных данных, содержащая актуальные для Учреждения угрозы информационной безопасности (т.е. угрозы, риск реализации которых является недопустимым), на основе которой вырабатываются требования, учитывающие особенности обработки персональных данных в Учреждении.

16.6. Необходимость использования средств криптографической защиты информации или шифровальных (криптографических) средств (далее — СКЗИ), предназначенных для защиты персональных данных при их обработке, хранении и передаче по каналам связи определяется Учреждением на основе результатов классификации и разработанной модели угроз информационной безопасности.

17. Ответственность за нарушения норм в сфере законодательства о персональных данных

17.1. Меры дисциплинарной ответственности

17.1.1. Должностные лица Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, привлекаются к дисциплинарной ответственности в порядке, установленном Трудовым кодексом РФ, трудовым договором.

В случаях однократного грубого нарушения должностным лицом Учреждения трудовых обязанностей, а именно: разглашения охраняемой законом тайны (служебной и иной), ставшей известной должностному лицу Учреждения в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого должностного лица, директор Учреждения вправе расторгнуть трудовой договор.

17.1.2. В рамках трудовых правоотношений в случае виновного противоправного поведения (действий или бездействия) сторон трудового договора в соответствии с Трудовым кодексом РФ, сторона трудового договора, причинившая ущерб другой стороне, возмещает этот ущерб.