Приложение № 1
к приказу ООО «Реабилитационный центр»
от 01.07.2017г №10-ОД

Положение об обработке персональных данных

1. Общие положения

1.1. Настоящее Положение предназначено для регулирования отношений, связанных с обработкой персональных данных, осуществляемой ООО «Реабилитационный центр» (Далее – Оператор) с использованием средств автоматизации, в том числе в информационнотелекоммуникационных сетях, и без использования таких средств, если обработка персональных данных соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и доступ к таким персональным данным.
1.2. Цель разработки Положения - определение порядка обработки персональных данных работников и иных субъектов персональных данных, персональные данные которых подлежат обработке, на основании полномочий Оператора; обеспечение защиты прав и свобод человека и гражданина, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.
1.3. Действие Положения распространяется на все персональные данные субъектов, обрабатываемые Оператором с применением средств автоматизации и без применения таких средств.
1.4. Настоящее Положение является локальным нормативным актом Оператора и вступает в силу с момента его утверждения руководителем и действует бессрочно, до замены его новым Положением.
1.5. Все изменения в Положение вносятся приказом Директора.
1.6. Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Оператора.
1.7. Цели обработки персональных данных:
- Кадровый учет работников (субъектов);
- Заключение и выполнение обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами;
- Регистрация и обработка сведений, необходимых для реализации полномочий ООО «МЦ МЕГИ»;
- Осуществление оказания медицинских услуг.
1.8. Основными законодательными и нормативно-правовыми актами Российской Федерации, регулирующие отношения, связанные с обработкой персональных данных Оператором, являются:

- Конституция Российской Федерации.
- Трудовой кодекс Российской Федерации от 30 декабря 2001 г. №197-ФЗ (ТК РФ).
- Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства Российской Федерации от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Закон РФ "О защите прав потребителя" от 07.02.1992 №2300-1;
- Закон «О государственной социальной помощи» №178-ФЗ от 17.07.1999;
- Постановление Правительства РФ от 04.10.2012 №1006 «Об утверждении правил предоставления медицинскими организациями платных медицинских услуг»;
- Федеральный закон от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан Российской Федерации»;
- Лицензия на осуществление медицинской деятельности;
- Устав общества и настоящее Положение.

2. Принципы обработки персональных данных

Обработка персональных данных Оператором осуществляется на законной и справедливой основе.

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. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

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

2.4. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки.

2.5. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность и актуальность по отношению к целям обработки персональных данных. Оператор принимает необходимые меры и обеспечивает их принятие по удалению и уточнению неполных и неточных данных.

2.6. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению с оформлением соответствующего акта либо обезличиванию по достижении целей.
2.7. Оператор и иные лица, получившие доступ к персональным данным, обязуются не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Основные понятия

В настоящем Положении используются следующие основные понятия:
3.1. персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
3.2. 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;
3.3. 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;
3.4. автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
3.5. распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
3.6. предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
3.7. блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
3.8. 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;
3.9. обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту

персональных данных;
3.10. информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
3.11. трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

4. Порядок обработки персональных данных субъектов по категориям

4.1. Персональные данные работников

4.1.1. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Обработка персональных данных работников Организации (получение, хранение, комбинирование, передача или любое другое использование персональных данных работника) осуществляется с целью обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества. Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации (Трудовой кодекс Российской Федерации от 30 декабря 2001 г. №197-ФЗ).
4.1.2. Информация, представляемая работником при поступлении на работу в организацию, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

– паспорт или иной документ, удостоверяющий личность;
– трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
– страховое свидетельство государственного пенсионного страхования;
– документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;
– документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
– свидетельство о присвоении ИНН (при его наличии у работника).

4.1.3. Перечень обрабатываемых персональных данных работников:
- фамилия, имя, отчество;
- пол;
- место, год и дата рождения;
- адрес по регистрации;

- адрес проживания (фактический);
- паспортные данные (серия, номер паспорта, кем и когда выдан);
- телефонный номер (домашний, рабочий, мобильный);
- семейное положение и состав семьи (муж/жена, дети);
- информация об образовании (наименование образовательного Организации, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- профессия;
- информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- ИНН;
- СНИЛС;
- данные об аттестации;
- данные о повышении квалификации и профессиональной переподготовке;
- данные о наградах, медалях, поощрениях, почетных званиях;
- справка о состоянии здоровья;
- информация о страховом свидетельстве государственного пенсионного страхования;
- информация о негосударственном пенсионном обеспечении;
- сведения о судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (для сотрудников осуществляющие организацию лечения несовершеннолетних);
- сведения о воинском учете (ФИО, категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета)
- данные о трудовом договоре (ФИО, № трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);

4.1.4. Способ получения персональных данных работника – персональные данные работника получаются у него самого, а также у третьих лиц в случае, оговоренном в п. 5.1.1. настоящего Положения.

4.1.5. Персональные данные работников обрабатываются как в бумажном, так и в электронном виде лицами согласно «Списку лиц, допущенных к обработке персональных данных», утвержденного руководителем Организации.

Типовые формы документов, содержащие персональные данные работников:

- Типовые формы первичной учетной документации по учету труда и его оплате, утвержденные законодательством Российской Федерации;
- Типовые формы бухгалтерского учета и отчетности, установленные законодательством Российской Федерации;
- типовые формы отчетности в ИФНС, ПФР, ФСС, утверждаемые соответствующими Приказами исполнительных органов данных учреждений;

Документы, содержащие персональные данные предоставляемые в военкоматы, по запросам правоохранительных органов и на основании других законных оснований, согласно п.5.1.4. настоящего Положения оформляются в свободной форме с указанием персональных данных в объеме, не превышающем законные требования.
4.1.6. Обработка персональных данных работников осуществляется для осуществления и выполнения, возложенных законодательством Российской Федерации на Организацию функций, полномочий и обязанностей. Передача персональных данных работников третьим лицам может осуществляться с согласия работника или в случаях, указанных в п. 5.1.4. настоящего Положения, включая в частности передачу персональных данных для целей налоговой отчетности, отчетности в ПФР, ФСС, передачу сведений в военкоматы о военнообязанных. Передача сведений в иные учреждения, организации и государственные органы осуществляется только с письменного указания Директора.
4.1.7. Сроки и условия обработки и хранения персональных данных
Обработка персональных данных осуществляется в течение трудовой деятельности работника.
Места хранения материальных носителей персональных данных определяются в соответствии с "Перечнем мест хранения".
Хранение персональных данных в электронном виде осуществляется в информационной системе персональных данных.
По расторжению трудового договора Организация осуществляет хранение персональных данных работника в соответствие со следующими сроками хранения:
Персональные данные работников содержащиеся в базах данных в электронном виде – до окончания срока сдачи персонифицированной отчетности установленной законодательством РФ. По окончания данного срока персональные данных должны быть уничтожены или обезличены в базах данных. Допускается хранение копий баз данных с персональными данными уволенных работников в электронном архиве в течение срока хранения и в объеме соответствующих бумажных документов.

Сроки хранения персональные данных работников, содержащихся в бумажных документах определены в номенклатуре дел организации.

4.1.8. По истечению срока хранения персональных данных работников персональные данные в электронных базах и бумажных носителях подлежат уничтожению.

4.2 Персональные данные пациентов

4.3.1. Обработка персональных данных пациентов ведется с целью оказания медицинских услуг.
Обработка персональных данных необходим для исполнения договора, стороной которого является субъект персональных данных.
Места хранения материальных носителей персональных данных определяются в соответствии с "Перечнем мест хранения".
Хранение персональных данных в электронном виде осуществляется в информационной системе персональных данных.
4.3.2. Состав персональных данных:

ФИО, паспортные данные, телефон, адрес, дата рождения, домашний адрес, место работы, должность, телефон, сведения о состоянии здоровья и др.
4.3.3. Персональные данные пациентов обрабатываются как в бумажном, так и в электронном виде, лицами согласно «Списку лиц, допущенных к обработке персональных данных», утвержденному Директором.
4.3.4. Сроки хранения персональных данных лиц, с которыми заключены договоры:
Срок хранения персональных данных пациентов Организации определяется в соответствии с номенклатурой дел организации.

4.3Персональные данные физических лиц-подрядчиков, физических лиц-поставщиков, физических лиц-дистрибьюторов, физических лиц-потребителей

4.4.1.Обработка персональных данных необходим для исполнения договора, стороной которого является субъект персональных данных.
4.4.2. Состав персональных данных: ФИО, СНИЛС, контактный номер телефона, реквизиты электронного ящика, сведения о начислениях, личные счета, адрес места проживания, паспортные данные, ИНН.
4.4.3. Персональные данные физических лиц-подрядчиков, лиц-поставщиков физических лиц-дистрибьюторов, физических лиц-потребителей обрабатываются как в бумажном, так и в электронном виде, лицами согласно «Списку лиц, допущенных к обработке персональных данных», утвержденному Директором. Хранение персональных данных в электронном виде осуществляется в информационной системе персональных данных.
4.4.4. Сроки хранения персональных данных лиц, с которыми заключены договоры:
Срок хранения персональных данных физических лиц-подрядчиков, лиц-поставщиков, физических лиц-дистрибьюторов, физических лиц-потребителей Организации определяется в соответствии с номенклатурой дел Организации.

5. Сбор персональных данных

5.1. Порядок получения персональных данных.
5.1.1. Все персональные данные работников Организации следует получать у них самих. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Организации должно сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.
5.1.2. Организация не имеет права получать и обрабатывать персональные данные работников об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни, сведений о состоянии здоровья, за исключением случаев, предусмотренных законодательством.
5.1.3. Организация как работодатель вправе обрабатывать персональные данные работников и прочих физических лиц только с их согласия, за исключением случаев, предусмотренных законодательством.
5.1.4. Согласие субъекта не требуется в следующих случаях:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- 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 (далее - исполнение судебного акта);
- обработка персональных данных необходима для предоставления государственной или муниципальной 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 персональных данных на едином портале государственных и муниципальных услуг;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения организационно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;
- обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года №8-ФЗ "О Всероссийской переписи населения";

- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных членов (участников) Организационного объединения или религиозной организации осуществляется соответствующими Организационным 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 без согласия в письменной форме субъектов персональных данных;
- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
- обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации,

законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

6. Порядок обработки персональных данных.

6.1. Субъект предоставляет должностному лицу Организации достоверные сведения о себе. Должностное лицо проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами.
6.2. Руководитель и работники Организации (операторы) при обработке персональных данных работника должны соблюдать следующие общие требования:
6.2.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, для оказания услуг клиентам, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
6.2.2. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными федеральными законами.
6.2.3. При принятии решений, затрагивающих интересы субъекта, Организация, как оператор, не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.
6.2.4. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Организацией как оператором за счет своих средств в порядке, установленном федеральным законом.
6.2.5. Работники и их представители должны быть ознакомлены под роспись с документами Организации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.
6.2.6. Во всех случаях отказ субъекта от своих прав на сохранение и защиту персональных данных недействителен.

7. Передача персональных данных

7.1. При передаче персональных данных субъекта Организация должна соблюдать следующие требования:
7.1.1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.
7.1.2. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.
7.1.3. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица,

получившие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.
7.1.4. Организация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. Лицо, осуществляющее обработку персональных данных по поручению Организации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом о персональных данных. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом о персональных данных. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции.
7.1.5. Не запрашивать у работников информацию об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.
7.1.6. Передавать персональные данные работников представителям в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

8. Доступ к персональным данным

8.1. Перечень лиц, имеющих право доступа к персональным данным, определяется «Списком лиц, допущенных к работе с персональными данными», утверждённым Директором Организации.
8.2. Субъект персональных данных, чьи персональные данные обрабатываются в информационной системе Организации имеет право:
8.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные этого субъекта.
8.2.2. Требовать от Организации уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для оператора персональных данных.
8.2.3. Получать от Организации:

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;
– сроки обработки персональных данных, в том числе сроки их хранения;
– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

8.2.4. Требовать извещения Организацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.2.5. Копировать и делать выписки персональных данных субъекта разрешается исключительно в служебных целях с письменного разрешения Директора.

8.3. Передача информации третьей стороне возможна только при письменном согласии субъектов.

9. Мероприятия по обеспечению безопасности персональных данных

9.1. Общие положения

9.1.1. Организация работ по обеспечению безопасности персональных данных осуществляется руководством Организации.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Организации, приказом Директора назначается лицо, ответственное за организацию обработки персональных данных.

Лицо, ответственное за организацию обработки персональных данных, в своей деятельности руководствуется нормативными документами в области обработки персональных данных.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных может осуществляться также сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

Лица, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании утвержденного списка.

Мероприятия по защите персональных данных осуществляются в соответствии с внутренним планом.

9.2. Мероприятия по обеспечению безопасности персональных данных при автоматизированной обработке.

9.2.1. Система защиты персональных данных

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

При обработке персональных данных в информационных системах Организации должно быть обеспечено:
- Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.
- Своевременное обнаружение фактов несанкционированного доступа к персональным данным.
- Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Постоянный контроль над обеспечением уровня защищенности информационной системы персональных данных.

9.2.2. Перечень мероприятий по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:
• Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз.
• Разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.
• Проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.
• Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией.
• Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.
• Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.
• Учет лиц, допущенных к работе с персональными данными в информационной системе.
• Контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
• Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
• Описание системы защиты персональных данных.

9.2.3. Определение уровня защищенности информационных систем персональных данных

Информационные системы персональных данных Организации подлежат обязательному определению уровня защищенности.

Для определения уровня защищенности информационных систем персональных

данных Организации приказом Директора Организации назначается комиссия.

Результаты определения уровня защищенности оформляются соответствующим актом.

9.2.4. Помещения, в которых ведется обработка персональных данных

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9.2.5. Лица, осуществляющие обработку персональных данных в автоматизированном виде, обязаны соблюдать требования «Инструкции пользователя информационной системы персональных данных» Организации.

9.3. Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации

9.3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

9.3.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

9.3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

9.3.4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

9.3.5. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

9.3.6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Организации или лица, осуществляющие такую обработку по договору с Организациям), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

9.3.7. При использовании типовых форм документов, характер информации в

которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:
а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Организации, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.
9.3.8. При ведении журналов, содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Организации, или в иных аналогичных целях, должны соблюдаться следующие условия:
а) необходимость ведения такого журнала должна быть предусмотрена «Положением о пропускном режиме», содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала, сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию Организации, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию Организации.
9.3.9. 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.
9.3.10. 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 (удаление, вымарывание).
9.3.11. Правила, предусмотренные пунктами 9.4.9, 9.4.10 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.
9.3.12. 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.
9.3.13. Лица осуществляющие неавтоматизированную обработку персональных данных обязаны соблюдать требования «Инструкции по обработке персональных данных без использования средств автоматизации» Организации.

10. Уничтожение персональных данных

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. Уничтожение персональных данных субъекта осуществляется комиссией с оформлением акта об уничтожении персональных данных.

11. Контроль и надзор за выполнением требований настоящего Положения

Контроль и надзор за выполнением требований настоящего Положения осуществляется в соответствии с «Планом внутренних проверок состояния защиты персональных данных».

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности, принятых мер. Он может проводиться ответственным за организацию обработки персональных данных, или на договорной основе

сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

12. Финансирование мероприятий по обеспечению безопасности персональных данных

Финансирование мероприятий по обеспечению безопасности персональных данных осуществляется за счет средств Организации.

13. Ответственность за нарушение требований настоящего положения

Лица, виновные в нарушении требований настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.