ООО «РГС-Медицина»

Положение
о порядке обработки персональных данных

Содержание

Термины, определения и сокращения

Сокращение	Полное наименование
ПДн	Персональные данные
ИСПДн	Информационная система персональных данных
СЗПДн	Система защиты персональных данных
Общество	ООО «РГС-Медицина»
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработки необходима для уточнения персональных данных)
Внешний/ съемный электронный носитель	Носители, существующие отдельно от средств вычислительной техники (СВТ) и подключающиеся к СВТ тем или иным способом, а также встроенные в корпус СВТ, в случае, если их можно извлечь (изъять) без вскрытия корпуса СВТ. В рамках данного документа под такими носителями понимаются флеш-карты; HDD - жесткие диски; оптические диски (CD, DVD и т.п.)
Договор ГПХ	Договор гражданско-правового характера.
Информационная система персональных данных	Информационная система, представляющая собой совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Конфиденциальность персональных данных	Обязанность Общества не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом
Обезличивание персональных данных	Действия, в результате которых невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

Обработка персональных данных	Любое действие (операция) или совокупность действий (операций», совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Общедоступные персональные данные	Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Распространение персональных данных	Действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Трансграничная передача персональных данных	Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу
Уничтожение персональных данных	Действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных

1 Общие положения

1.1 Назначение документа

1.1.1. Настоящее Положение устанавливает единые требования к проведению мероприятий по обработке и защите персональных данных в ООО «РГС-Медицина» (далее – Общество):

- определяет общие принципы, требования и порядок обработки и защиты персональных данных в структурных подразделениях Общества в целях защиты прав субъектов ПДн (работников Общества и застрахованных лиц);
- служит основной для обеспечения соответствия процессов обработки персональных данных в структурных подразделениях Общества требованиям действующего законодательства РФ;
- определяет требования и устанавливает порядок контроля над деятельностью по обработке и защите персональных данных от несанкционированного доступа, неправомерного их использования или утраты в структурных подразделениях Общества.

1.2 Правовые и нормативно-методические источники документа

1.2.1. Настоящее Положение разработано в соответствии со следующими нормативно-правовыми документами:

- Статья 24 Конституции Российской Федерации;
- Глава 14 Трудового Кодекса Российской Федерации;
- Федеральный закон Российской Федерации №152-ФЗ «О персональных данных» от 27.07.2006 г.;
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3 Область действия документа

1.3.1. Положения настоящего документа обязательны для исполнения всеми работниками Общества и третьими сторонами, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования по защите персональных данных (после ознакомления под подпись).

1.3.2. Действие Положения распространяется на структурные подразделения Общества, филиалы Общества и офисы, зарегистрированные Обществом в установленном законодательством РФ порядке

1.4 Область применения документа

1.4.1. Положение применяется при реализации технологических и бизнес-процессов, в соответствии с которыми в Обществе осуществляется обработка персональных данных. К таким процессам относятся:

1.4.1.1. Процессы, связанные с обработкой персональных данных застрахованных по ОМС лиц, в т.ч.:

- оформление заявления о выборе (замене) страховой медицинской организации;
- оформление заявления о выдаче полиса (выдаче дубликата полиса), переоформлении полиса обязательного медицинского страхования;
- информирование застрахованных лиц в письменной форме о факте страхования и необходимости получения полиса обязательного медицинского страхования;
- оформление (переоформление), выдача полиса обязательного медицинского страхования застрахованному лицу;
- предоставление территориальному фонду данных о новых застрахованных лицах и сведений об изменении данных о ранее застрахованных лицах;
- ведение учета застрахованных лиц, выданных им полисов обязательного медицинского страхования в соответствии с порядком персонифицированного учета в сфере обязательного медицинского страхования;
- составление с территориальным фондом актов сверки численности застрахованных лиц;
- осуществление контроля объема, сроков, качества и условий предоставления медицинской помощи застрахованным лицам в медицинских организациях и представление отчетов о результатах контроля;
- сбор, обработка, обеспечение сохранности и конфиденциальности сведений и информации при осуществлении персонифицированного учета сведений о застрахованных лицах и персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам,
- осуществление обмена указанными сведениями и информацией между субъектами ПДн и участниками обязательного медицинского страхования.

1.4.1.2. Процессы, связанные с обработкой персональных данных работников Общества в соответствии с Трудовым кодексом и другими нормативными правовыми актами Российской Федерации.

1.4.1.3. Процессы, связанные с обработкой персональных данных соискателей должностей Общества.

1.4.1.4. Процессы передачи (хранения) дел в архив и ведение архивного дела.

1.5 Порядок ввода в действие и изменение Положения

1.5.1. Настоящее Положение вступает в силу с момента его утверждения приказом Общества.

1.5.2. Все изменения в Положение утверждаются приказом Общества.

2 Субъекты персональных данных, состав обрабатываемых персональных данных

2.1. В Обществе обрабатываются персональные данные следующих субъектов ПДн:

- физических лиц – клиентов Общества, являющихся застрахованными по ОМС лицами;
- работников Общества, работающих по трудовым договорам и договорам возмездного оказания услуг;
- соискатели должностей;
- физических лиц - состоящих в договорных и иных гражданско-правовых отношениях с Обществом.

2.2. Состав и местонахождение персональных данных клиентов Общества, застрахованных по ОМС физических лиц

2.2.1. Состав персональных данных застрахованных по ОМС лиц установлен Федеральным законом от 29.10.2010 г № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».

2.2.2. В состав персональных данных при ведении персонифицированного учета сведений о застрахованных лицах , входят:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета (СНИЛС), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;
- номер полиса обязательного медицинского страхования застрахованного лица;

- данные о страховой медицинской организации, выбранной застрахованным лицом;
- дата регистрации в качестве застрахованного лица;
- статус застрахованного лица (работающий, неработающий).

2.2.3. В состав персональных данных при ведении персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам**,** входят:

- номер полиса обязательного медицинского страхования застрахованного лица;
- медицинская организация, оказавшая соответствующие услуги;
- виды оказанной медицинской помощи;
- условия оказания медицинской помощи;
- сроки оказания медицинской помощи;
- объемы оказанной медицинской помощи;
- стоимость оказанной медицинской помощи;
- диагноз;
- профиль оказания медицинской помощи;
- медицинские услуги, оказанные застрахованному лицу, и примененные лекарственные препараты;
- примененные медико-экономических стандарты;
- специальность медицинского работника, оказавшего медицинскую помощь;
- результат обращения за медицинской помощью;
- результаты проведенного контроля объемов, сроков, качества и условий предоставления медицинской помощи**.**

2.2.4. Персональные данные застрахованных по ОМС физических лиц содержатся:

- в типовых формах документов (заявления, журналы, уведомления, акты, формируемые по результатах контроля объема, сроков, качества и условий предоставления медицинской помощи застрахованным лицам в медицинских организациях), характер информации в которых в соответствии с законодательством РФ в сфере ОМС предполагает или допускает включение в них персональных данных,
- в письменных обращениях застрахованных лиц в адрес Общества;
- в счетах-реестрах, предоставляемых на оплату в структурные подразделения Общества;

- в информационных системах персональных данных (ИСПДн), используемых Обществом при ведении персонифицированного учета застрахованных лиц и оказанной им медицинской помощи.

2.3. Состав и местонахождение персональных данных работников Общества

2.4.1. В состав персональных данных работников Общества входят:

- 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 работника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- страховой номер индивидуального лицевого счета (СНИЛС);
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки работников;
- 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.

2.4.2. Персональные данные работников Общества содержатся в документах персонального учета работников, финансовой документации, а также в иных документах, формируемых в процессе осуществления профессиональной деятельности Дирекции по работе с персоналом Общества и подразделений, осуществляющих бухгалтерский учет (в т.ч. бухгалтериях филиалов Общества). Персональные данные работников содержатся также в

информационных системах Общества, доступ к которым предоставлен ограниченному кругу работников Общества (в том числе региональных подразделений) в соответствии с выполняемыми должностными обязанностями.

2.4. Состав и местонахождение персональных физических лиц - состоящих в договорных и иных гражданско-правовых отношениях с Обществом

2.5.1. В состав персональных данных работников – физических лиц, состоящих в договорных и иных гражданско-правовых отношениях с Обществом, входят:

- ФИО;
- дата рождения;
- место рождения;
- пол;
- данные документов, удостоверяющих личность;
- ИНН (при наличии);
- страховой номер индивидуального лицевого счета (СНИЛС),
- адрес регистрации по месту жительства/адрес фактического проживания;
- гражданство;
- контактные данные (контактный телефон; адрес электронной почты);
- место работы и должность.

2.5.2. Персональные данные указанной категории субъектов ПДн содержатся в заключаемых с ними договорах, документах, относящихся к исполнению данных договоров, и ИСПДн, используемых Обществом при исполнении обязательств, предусмотренных заключенными договорами.

2.5. Состав и местонахождение персональных данных соискателей должностей Общества

2.6.1. В состав персональных соискателей должностей Общества, входят:

- ФИО;
- дата рождения;
- семейное положение;
- адрес регистрации по месту жительства/адрес фактического проживания;
- образование;
- опыт работы;
- контактные данные (контактный телефон; адрес электронной почты).

2.6.2. Персональные данные указанной категории субъектов ПДн содержатся в резюме/анкетах.

3 Цели и правовое основание обработки персональных данных

3.1. Обработка персональных данных физических лиц, застрахованных по ОМС, осуществляется в целях исполнения обязательств страховой медицинской организации, предусмотренных Федеральным законом от 29.10.2010 г № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Правил ОМС (утв. Приказом Минздравсоцразвития РФ от 28.12.2010 г № 1219н), типового договора о финансовом обеспечении обязательного медицинского страхования (утв. Приказом Минздравсоцразвития 24.12.2010 г № 1185н), типового договора на оказание и оплату медицинской помощи по обязательному медицинскому страхованию (утв. Приказом Миздравсоцразвития РФ от 24.12.2010 г 3 1184н) , других нормативных правовых актов РФ , регулирующих взаимодействие субъектов ПДн и участников системы ОМС, а также в целях обеспечения выполнения работ и предоставления услуг, определенных Уставом и лицензиями Общества .

3.2. Обработка персональных данных субъектов ПДн, являющихся работниками Общества, осуществляется в целях регулирования трудовых отношений между Обществом и работниками, содействия работникам в выполнении ими своих функциональных обязанностей, обучении, карьерного продвижения по работе, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Общества, очередности предоставления отпусков, установления и расчета размера заработной платы, страхования работников, оформления страховых свидетельств государственного пенсионного страхования и обязательного медицинского страхования, обеспечения пропускного режима Общества и безопасности сотрудников, учета времени, проведенного работником в помещении Общества, а также в иных целях, необходимых Обществу в связи с трудовыми отношениями с работниками Общества, в т.ч. соблюдением корпоративной культуры Общества (в части ведения телефонного справочника).

3.3. Обработка персональных данных субъектов ПДн, работающих по договорам ГПХ, осуществляется в целях контроля количества и качества выполняемой работы, выполнения договорных обязательств Общества перед субъектом ПДн (в т.ч. в части оплаты услуг), обеспечения пропускного режима Общества.

3.4. Обработка персональных данных субъектов ПДн, являющихся соискателями должностей, осуществляется с целями принятия решения о возможности заключения с ними трудового договора.

4 Общие положения по обработке персональных данных

4.1 Общие требования

4.1.1 Обработка и обеспечение безопасности персональных данных в Обществе осуществляется в соответствии с требованиями Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона № 152-ФЗ «О персональных данных», подзаконных актов, других определяющих случаи и особенности обработки персональных данных федеральных законов, руководящих и методических документов ФСТЭК России и ФСБ России.

4.1.2 При обработке персональных данных Общество придерживается следующих основных принципов:

- Общество осуществляет обработку персональных данных только на законной и справедливой основе;
- Общество не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта ПДн (если иное не предусмотрено действующим законодательством Российской Федерации);
- Общество определяет конкретные законные цели до начала обработки (в т.ч. сбора) персональных данных;
- Общество собирает только те персональные данные, которые являются необходимыми и достаточными для заявленной цели обработки;
- обработка персональных данных в Обществе ограничивается достижением конкретных, заранее определенных и законных целей.

4.1.3 Общество не осуществляет сбор и обработку персональных данных граждан, касающихся расовой, национальной принадлежности, политических, религиозных, философских и иных убеждений, интимной жизни, членства в общественных объединениях, в том числе в профессиональных союзах.

4.1.4 В случаях, установленных законодательством Российской Федерации, Общество вправе осуществлять передачу персональных данных субъектов ПДн. Передача персональных данных осуществляется в соответствии с требованиями законодательства Российской Федерации в части обработки и защиты персональных данных.

4.1.5 Общество вправе поручить[1] обработку персональных данных (с согласия субъекта ПДн) третьим лицам, на основании заключаемого с этими лицами договора (поручения).

4.1.6 Лица, осуществляющие обработку персональных данных по поручению Общества, обязуются соблюдать принципы и правила обработки и защиты персональных данных, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных». Для каждого третьего лица в договоре (поручении) определяется перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, устанавливается обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, также указываются требования к защите обрабатываемых персональных данных.

4.1.7 Обработка (сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) персональных данных подразделяется на:

- обработку персональных данных в информационных системах персональных данных с использованием средств автоматизации;
- обработку персональных данных, осуществляемую без использования средств автоматизации.

4.2 Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации

4.2.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких 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 ИСПД».

4.2.2. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

[1] Если иное не предусмотрено федеральным законом.

- если не обеспечена конфиденциальность указанных данных (за исключением обезличенных персональных данных и в отношении общедоступных персональных данных);
- при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных и регламента предоставления доступа к данным информационной системы.

4.3 Обработка персональных данных, осуществляемая без использования средств автоматизации

4.3.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека.

4.3.2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

4.3.3. 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 (т.е., например, хранение материальных носителей персональных данных с целью осуществления страховой деятельности и с целью кадрового учета должны проводиться отдельно).

4.3.4. Дополнительно, при неавтоматизированной обработке персональных данных на бумажных носителях:

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, должны формироваться в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

4.3.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Общества или лица, осуществляющие такую обработку по договору с Обществом), должны быть проинформированы о факте обработки ими персональных данных, осуществляемой Обществом без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами, в том числе, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Общества (при их наличии).

4.3.6. При использовании типовых форм документов, разработанных в Обществе, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- 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; имени (наименовании) и адреса Общества или структурного подразделения Общества; фамилию, имя, отчество и адрес субъекта ПДн; источник получения персональных данных; сроки обработки персональных данных; перечень действий с персональными данными, которые будут совершаться в процессе их обработки; общее описание используемых Обществом способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, в случае необходимости получения письменного согласия на обработку персональных данных;
- 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;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.3.7. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный 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:

- 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 применяется (распространяется) копия персональных данных;
- 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.

4.3.8. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых шкафах, ящиках столов, сейфах. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

4.3.9. В помещениях, предназначенных для хранения документов и внешних электронных носителей информации, содержащие персональные данные (материальные носители персональных данных) и работы с ними, запрещается нахождение посторонних лиц[2] без присутствия работников Общества, работающих в указанных помещениях (или имеющих право доступа в эти помещения). При этом работники Общества должны контролировать действия посторонних лиц, не допуская получения такими лицами доступа к материальным носителям персональных данных (в случае, если доступ к материальным носителям персональных данных им запрещен).

4.3.10. За сохранность конкретного материального носителя персональных данных отвечает работник, получивший этот материальный носитель персональных данных в пользование.

4.3.11. В целях обеспечения сохранности и безопасности материальных носителей персональных данных работникам Общества запрещается:

- разглашать содержимое материальных носителей персональных данных;

[2] Здесь и далее: под «посторонними лицами» следует понимать любых лиц, не работающих/не имеющих права доступа в эти помещения.

- передавать материальные носители персональных данных лицам, не имеющим права доступа к ним;
- несанкционированно вносить какие-либо изменения в материальные носители персональных данных;
- использовать материальные носители персональных данных, подлежащие уничтожению;
- оставлять материальные носители персональных данных на столах и в других легкодоступных местах при отсутствии работника на рабочем месте;
- несанкционированно копировать и/или тиражировать материальные носители персональных данных;
- выносить материальные носители персональных данных за пределы служебных помещений. В случаях, когда необходимость выноса определена рабочим процессом, вынос осуществляется на основании письменного разрешения руководителя структурного подразделения.

4.3.12. При печати персональных данных на материальные носители:

- запрещается оставлять материальные носители в принтере после печати;
- работник, уходящий последним из кабинета, должен убедиться, что в принтере отсутствуют материальные носители персональных данных. В случае обнаружения материальных носителей персональных данных в принтере указанный работник должен сообщить о данном факте своему непосредственному руководителю.

4.3.13. Передача материальных носителей персональных данных между подразделениями Общества может осуществляться только между работниками, структурные подразделения которых включены в «Перечень подразделений, работники которых имеют доступ к персональным данным».

4.3.14. Уточнение персональных данных на материальном носителе производится путем фиксации на том же материальном носителе сведений о вносимых в него изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными и уничтожением старого.

4.3.15. 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).

4.3.16. Уничтожение материальных носителей персональных данных производится специально назначаемой комиссией с оформлением актов об уничтожении.

4.3.17. При увольнении работника, имеющего доступ к материальным носителям персональных данных, он обязан сдать все имеющиеся у него материальные носители персональных данных, полученные/созданные им в ходе выполнения должностных обязанностей, руководителю подразделения.

4.3.18. О фактах утраты материальных носителей персональных данных, либо разглашения содержащихся в них сведений, либо обнаружения других признаков инцидентов информационной безопасности необходимо немедленно поставить в известность непосредственного руководителя.

4.3.19. Ведение журналов, содержащих персональные данные, необходимые для однократного пропуска субъекта ПДн на территорию Общества (в т.ч. на территорию региональных подразделений/филиалов), может осуществляться в случае, если отсутствует система контроля доступа. Форма Журнала приведена в Приложении 1.

4.3.20. Для ведения журналов, указанных в п.4.3.19, должны выделяться лица, ответственные за ведение и сохранность журналов. При ведении подобного журнала должны соблюдаться следующие условия:

- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию, на которой находится Общество.

Примечание. В случае, если субъект ПДн проходит на территорию, на которой осуществляется обслуживание клиентов и/или нет возможности выделить работника для ведения журнала в связи с малой численностью персонала подразделения и отсутствием сотрудников охраны (в случае небольших агентств), ведение журналов не является необходимым.

5 Основные этапы жизненного цикла персональных данных

5.1 Получение персональных данных

5.1.1. Получение персональных данных субъекта ПДн возможно как у него самого, так и из других источников.

При этом, если Общество может получить необходимые персональные данные субъекта ПДн только у третьей стороны, Общество должно уведомить об этом субъекта ПДн (за исключением случаев, предусмотренных законодательством), сообщив следующую информацию:

- наименование и адрес Общества;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные федеральным законом права субъекта ПДн;
- источник получения персональных данных

и получить от него письменное согласие.

5.1.2. Согласия субъекта ПДн на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта ПДн на передачу его персональных данных третьим лицам получено от него в письменной форме при заключении договора с Обществом (только персональных данных, указанных в договоре), а также в случаях, установленных Федеральным законом № 152-ФЗ «О персональных данных».

5.1.3. Если обязанность предоставления персональных данных установлена федеральным законом, Общество обязано разъяснить субъекту ПДн юридические последствия отказа предоставить свои персональные данные.

5.1.4. Общество имеет право проверять достоверность сведений, предоставленных субъектом ПДн (всех категорий), сверяя данные, предоставленные субъектом ПДн, с имеющимися у Общества документами.

5.1.5. Общество не вправе обрабатывать персональные данные субъекта ПДн без его письменного согласия, за исключением следующих случаев (п.2 ст.6 Федерального закона №152-ФЗ «О персональных данных»):

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов ПДн, персональные данные которых подлежат обработке, а также определяющего полномочия Общества (Примечание. Обработка персональных данных в системе ОМС осуществляется на основании Федерального закона от

29.11.2010 г № 326-Фз «Об обязательном медицинском страховании в Российской Федерации»);

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации;
- обработка персональных данных осуществляется в целях исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- обработка персональных данных осуществляется для статистических или иных исследовательских целях (за исключением обработки персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации) при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе (общедоступные персональные данные);
- обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- 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.

5.1.6. Письменное согласие субъекта ПДн должно включать:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Общества, получающего согласие субъекта ПДн;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Обществом способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва, если иное не установлено федеральным законом;
- подпись субъекта ПДн.

5.1.7. Запрещается получать и иным способом обрабатывать персональные данные субъекта ПДн, касающиеся расовой, национальной принадлежности, политических, религиозных, философских и иных убеждений, состояния здоровья, интимной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

5.1.8. Общество вправе получать и обрабатывать персональные данные, указанные в настоящем пункте только в следующих случаях:

- субъект ПДн дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные сделаны общедоступными субъектом ПДн;
- обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- 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 ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;
- обработка персональных данных необходима для установления или осуществления прав субъекта ПДн 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-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка полученных в установленном законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

5.1.9. При изменении персональных данных субъект ПДн (физические лица, застрахованные по ОМС, работники Общества и др.) уведомляет Общество о таких изменениях. Данное обязательство не распространяется на изменение персональных данных, предоставление которых требует соответствующее согласие работника.

5.2 Хранение персональных данных

5.2.1. Персональные данные субъектов ПДн на бумажных носителях хранятся:

- в подразделениях Общества, на которые возложена функция регистрации граждан в качестве застрахованных в системе ОМС лиц, выдачи им полисов ОМС, ведения учета застрахованных лиц и ввода данных о застрахованных лицах в ИСПДн;
- в подразделениях Общества, на которые возложена функция осуществления защиты прав застрахованных по ОМС лиц и проведения контроля объема, сроков, качества и условий предоставления медицинской помощи застрахованным лицам в медицинских организациях;
- в Дирекции по работе с персоналом, в подразделениях филиалов, осуществляющих кадровое делопроизводство;

- в Дирекции технологий ОМС;
- в Дирекции по организации ОМС;
- в Дирекции по ЗПЗ и ЭКМП;
- в подразделениях, на которые возложены функции заключения договоров страхования и ввода их в ИСПДн,
- в подразделениях, на которые возложены функции расчета заработной платы работников Общества (Бухгалтерия ЦО), в бухгалтериях филиалов;
- в подразделениях Общества, которые отвечают за взаимодействие с субъектами ПДн, не являющихся работниками Общества.

5.2.2. Персональные данные субъектов ПДн хранятся:

- в бумажном виде в папках в помещениях подразделений в надежно запираемых шкафах, ящиках столов, сейфах, обеспечивающих защиту от несанкционированного доступа;
- в электронном виде в ИСПДн. Доступ к ИСПДн, содержащим персональные данные, обеспечивается использованием средств защиты от несанкционированного доступа и копирования.

5.2.3. Помещения, где осуществляется хранение и обработка персональных данных, должны отвечать требованиям, обеспечивающим их сохранность (Приложение № 7). В частности, размещение указанных помещений должно исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в этих помещениях документов.

5.2.4. Учет внешних (съемных) электронных носителей информации, содержащей персональные данные, осуществляется в структурных подразделениях, обрабатывающих указанные персональные данные, в соответствии с требованиями п. 5.2.9 настоящего документа.

5.2.5. Работник, имеющий доступ к персональным данным работников Общества в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные, исключающее доступ к ним третьих лиц;
- при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте он обязан передать документы и иные носители, содержащие персональные данные, лицу, на которое возложено исполнение его трудовых обязанностей на время его отсутствия.

Примечание. В случае если такое лицо не назначено, документы и иные носители, содержащие персональные данные, передаются другому работнику, имеющему надлежащим образом оформленный, в соответствии с п. 5.4.1. настоящего документа, доступ к персональным данным, по указанию руководителя структурного подразделения.

5.2.6. При увольнении работника, имеющего доступ к персональным данным субъекта ПДн, документы и иные носители, содержащие указанные персональные данные, сдаются руководителю структурного подразделения.

5.2.7. Оперативный контроль за организацией работ с документами и исключение несанкционированного доступа к ним возлагается на Руководителя структурного подразделения.

5.2.8. Хранение персональных данных субъектов ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки и нормативные документы, регулирующие страховую деятельность.

5.2.9. Учет внешних/съемных электронных носителей персональных данных осуществляется в следующем порядке:

5.2.9.1. В Обществе запрещено использовать флэш-карты, внешние жесткие диски, оптические диски, дискеты для хранения и обработки персональных данных. Персональные данные должны обрабатываться и храниться в ИСПДн. В виде исключения, возможно, использовать внешний носитель, как временное хранение в целях исполнения поручения руководства Общества для сотрудников ЦО по согласованию с Генеральным директором и Директором Дирекции по информационным технологиям, для сотрудников филиала - по согласованию с директором филиала.

5.2.9.2. В Обществе должны быть учтены все внешние/съемные электронные носители информации, на которых хранятся резервные копии (ленточные накопители, ленточные библиотеки, диски сетевого хранилища данных).

5.2.9.3. Кандидатуры работников, на которых планируется возложить обязанности по учету носителей с персональными данными в филиалах Общества, должны назначаться распоряжением по филиалу.

5.2.9.4. Первоначальная инвентаризация носителей осуществляется в каждом структурном подразделении Общества, имеющем доступ к персональным данным силами работников подразделений.

5.2.9.5. Каждому носителю персональных данных присваивается учетный номер. Для этого все носители должны быть учтены по серийным номерам, либо при отсутствии таковых, наклейкой с инвентарным номером.

5.2.9.6. Учет носителей осуществляется по Журналу учета носителей персональных данных. Форма Журнала приведена в Приложении 2.

5.2.9.7. Инвентаризация всех носителей информации, на которых хранятся персональные данные, должна осуществляться в каждом структурном подразделении, осуществляющем обработку персональных данных, не реже 1 раза в год работником, назначаемым руководителем структурного подразделения. Результаты инвентаризации должны документироваться (отражаться в Акте), который утверждается руководителем структурного подразделения и передается на хранение в Дирекцию по информационным технологиям.

5.3 Использование персональных данных

5.3.1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением (п. 2 ст.16 Федерального закона №152-ФЗ «О персональных данных») следующих случаев:

- в случае наличия согласия в письменной форме субъекта ПДн;
- в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

5.3.2. Общество обязано разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.

5.3.3. Общество обязано рассмотреть возражение, указанное в п. 5.3.2 настоящего документа, в течение тридцати рабочих дней со дня его получения и уведомить субъекта ПДн о результатах рассмотрения такого возражения.

5.4 Доступ к персональным данным и передача персональных данных субъектов ПДн

5.4.1 Организация допуска к персональным данным

5.4.1.1. Доступ к персональным данным субъекта ПДн имеют работники Общества, которым персональные данные необходимы в связи с исполнением ими трудовых

обязанностей. Перечень подразделений, работники которых имеют доступ к персональным данным, определяется Генеральным директором по представлению заместителей и руководителей структурных подразделений Общества и утверждается приказом по Обществу.

5.4.1.2. Доступ к персональным данным субъектов ПДн работникам Общества, не включенным в указанный выше перечень, может быть предоставлен в целях выполнения порученного задания и на основании служебной записки с положительной резолюцией Генерального директора. Служебная записка должна содержать объем и срок предоставления доступа. Служебная записка может быть оформлена в электронном виде, исключающем подмену оригинала.

5.4.1.3. В случае, если Обществу оказывают услуги юридические и физические лица на основании заключенных договоров, в силу которых им может быть предоставлен доступ к конфиденциальной информации (в т.ч. к персональным данным субъектов ПДн), то до начала работ должно быть подписано соглашение о неразглашении конфиденциальной информации между Обществом и указанными физическими или юридическими лицами, либо положения о неразглашении конфиденциальной информации должны быть включены в текст соответствующих договоров с указанными физическими и юридическими лицами. Текст соглашения о неразглашении должен содержать положения об обеспечении указанными лицами конфиденциальности и безопасности персональных данных при их обработке, а также правила, устанавливающие порядок обработки персональных данных.

5.4.1.4. Процедура оформления допуска к персональным данным включает в себя:

- принятие на себя обязательств перед Обществом по нераспространению доверенных им сведений, составляющих конфиденциальную информацию (отражаются в трудовом договоре). В случае, если работнику оформляется допуск на основании служебной записки – истребование с работника письменного обязательства о соблюдении конфиденциальности персональных данных субъектов ПДн и соблюдении правил их обработки;
- ознакомление работника под подпись с порядком и правилами обработки персональных данных в Обществе;
- допуск оформляемого лица к ПД в ИСПДн осуществляется только в соответствии требованиями Регламента предоставления доступа (наличие регламента предоставления доступа к ИСПДн является обязательным требованием сдачи и приема ИСПДн в промышленную эксплуатацию).

5.4.1.5. Доступ к персональным данным субъектов ПДн без специального разрешения (без оформления служебной записки в соответствии с п. 5.4.1.4) имеют работники, занимающие в Обществе следующие должности:

- Генеральный директор;
- работники Дирекции по информационным технологиям;
- субъекты ПДн (только к своим персональным данным).

5.4.1.6. Доступ к персональным данным субъектов ПДн других работников Общества, не имеющих надлежащим образом оформленного допуска, запрещается.

5.4.2 Доступ к персональным данным

5.4.2.1. Общество обеспечивает конфиденциальность персональных данных субъектов ПДн, то есть не допускает их распространение без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

5.4.2.2. В отношении персональных данных субъектов ПДн вводится режим ограничения доступа. Доступ к персональным данным субъекта ПДн должны иметь только те работники Общества, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей и только в необходимом объеме.

5.4.2.3. Лица, имеющие внутренний доступ к персональным данным субъектов ПДн, обязаны соблюдать режим конфиденциальности персональных данных.

5.4.2.4. Работники Общества, участвующие в обработке персональных данных, должны быть ознакомлены под подпись с документами Общества, устанавливающими порядок обработки персональных данных субъектов ПДн, а также об их правах и обязанностях в этой области.

5.4.2.5. Субъект ПДн имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев, предусмотренных п.5 ст.14 Федерального закона №152-ФЗ «О персональных данных»), содержащей его персональные данные. Субъект ПДн имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

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

- подтверждение факта обработки персональных данных Обществом;
- сведения о правовых основаниях и целях такой обработки;
- сведения о способах обработки персональных данных, применяемых Обществом;

- сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона;
- перечень обрабатываемых персональных данных и источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
- сведения о сроках обработки персональных данных, в том числе сроках их хранения;
- сведения о порядке осуществления субъектом ПДн прав, предусмотренных законодательством о персональных данных;
- наименование и адрес лица, осуществляющего обработку персональных данных по поручению Общества;
- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его персональных данных;
- иные сведения, предусмотренные законодательством Российской Федерации.

5.4.2.7. Субъект ПДн – работник Общества получает доступ к своим персональным данным по запросу в Дирекцию по работе с персоналом. При получении подобного запроса работники Дирекции по работе с персоналом в течении 3-х рабочих дней формируют ответ на запрос.

5.4.2.8. Доступ к своим персональным данным предоставляется субъекту ПДн, не являющемуся работником Общества или его законному представителю при обращении, либо при получении запроса субъекта ПДн или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных и собственноручную подпись субъекта ПДн или его законного представителя.

5.4.2.9. Обработка обращений (запросов) субъектов ПДн, не являющихся работниками Общества или их законных представителей осуществляется работниками Юридической службы с привлечением представителей подразделений, отвечающих (отвечавших) за взаимодействие с указанным субъектом ПДн.

5.4.2.10. Учет обращений субъектов ПДн осуществляется в соответствии со следующими правилами:

- учет обращений работников Общества ведется в Дирекции по работе с персоналом в соответствии с «Положением о порядке обработки персональных данных работников»;
- учет обращений субъектов ПДн, не являющихся работниками Общества (или их законных представителей) ведется в соответствии с инструкциями по делопроизводству, принятыми в Обществе и осуществляется путем ведения Журнала учета обращений (Приложение 3).

5.4.3 Передача персональных данных субъекта ПДн третьим лицам

5.4.3.1. При передаче персональных данных субъекта ПДн Общество придерживается следующих требований:

1) Передача персональных данных субъекта ПДн третьим лицам осуществляется только с письменного согласия субъекта ПДн (сведения, которые должны содержаться в письменном согласии субъекта ПДн, определяются п. 5.1.6 настоящего документа), за исключением случаев, установленных федеральными законами.

Примечание: Согласия субъекта ПДн на обработку (в т.ч. передачу) его персональных данных третьим лицам не требуется в случаях, предусмотренных Федеральным законом №152-ФЗ «О персональных данных».

2) Не допускается передача персональных данных субъекта ПДн в целях продвижения товаров, работ, услуг на рынке без его согласия.

3) Передача третьим лицам документов (иных материальных носителей), содержащих персональные данные субъектов ПДн, осуществляется по письменному запросу третьего лица на предоставление персональных данных субъекта ПДн.

4) Работники Общества, передающие персональные данные субъектов ПДн третьим лицам, должны передавать их с обязательным уведомлением лица, получающего эти документы, об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена, и с предупреждением об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами. Уведомление и предупреждение могут быть реализованы путем подписания акта передачи носителей персональных данных, в котором приведены указанные условия. Типовая форма Акта приведена в Приложении 4.

- Представителю субъекта ПДн (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством Российской Федерации и настоящим документом. Информация передается при

наличии нотариально удостоверенной (или приравненной к нотариально удостоверенной) доверенности представителя субъекта ПДн.

Доверенности и заявления хранятся в личном деле субъекта ПДн.

5) Предоставление персональных данных субъекта ПДн уполномоченному органу по защите прав субъектов ПДн, на который возлагаются функции обеспечения контроля и надзора за соответствием обработки персональных данных требованиям ФЗ №-152, осуществляется по запросу (указанный уполномоченный орган имеет право запрашивать у Общества информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию).

6) Предоставление персональных данных субъекта ПДн государственным органам производится в соответствии с требованиями действующего законодательства Российской Федерации.

7) Персональные данные субъекта ПДн могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта ПДн, за исключением случаев, когда передача персональных данных субъекта ПДн без его согласия допускается действующим законодательством Российской Федерации.

5.4.3.2. Учет переданных персональных данных осуществляется в рамках принятых в Обществе правил делопроизводства путем регистрации входящей и исходящей корреспонденции и запросов как государственных органов, так и структурных подразделений Общества, физических (юридических) лиц либо их представителей о предоставлении персональных данных. Фиксируются сведения о лицах, направивших такие запросы, дата выдачи персональных данных, а также дата уведомления об отказе в предоставлении персональных данных (в случае отказа).

5.4.3.3. В случае если лицо, обратившееся в Общество с запросом на предоставление персональных данных, не уполномочено на получение информации, относящейся к персональным данным, Общество обязано отказать лицу в выдаче такой информации. Лицу, обратившемуся с соответствующим запросом, выдается уведомление в свободной форме об отказе в выдаче информации, а копия уведомления хранится в соответствии с принятыми правилами делопроизводства (как исходящая корреспонденция). В случае если запрашивались персональные данные работника Общества, копия уведомления также подшивается в личное дело работника, персональные данные которого не были предоставлены.

5.5 Блокирование персональных данных

5.5.1. В случае выявления неточных[3] персональных данных субъекта ПДн или неправомерных действий с ними работников Общества при обращении или по запросу субъекта ПДн или его законного представителя либо уполномоченного органа по защите прав субъектов ПДн осуществляется блокирование[1] персональных данных, относящихся к соответствующему субъекту ПДн, с момента такого обращения или получения такого запроса на период проверки.

5.5.2. Блокирование (временное прекращение обработки персональных данных и запрет на передачу персональных данных в сторонние организации) персональных данных по факту обработки недостоверных персональных данных субъекта ПДн или неправомерных действий с ними работников Общества утверждается приказом в ЦО по факту произошедшему в ЦО и в Филиале по факту произошедшему в региональном подразделении.

5.5.3. Приказ должен быть согласован с Юридической службой, Дирекцией по информационным технологиям и доведен до сведения причастных руководителей структурных подразделений Общества о необходимости блокирования персональных данных (временном прекращении обработки персональных данных в части запрета на передачу персональных данных в сторонние организации) соответствующего субъекта ПДн. Руководители структурных подразделений Общества, в свою очередь, оповещают причастных работников своих подразделений о блокировании данных.

5.5.4. Блокирование персональных данных субъекта ПДн производится ответственным работником подразделения информационных технологий внутренними средствами ИСПДн на основании Приказа.

5.5.5. В случае подтверждения факта недостоверности персональных данных субъекта ПДн на основании документов, представленных субъектом ПДн или его законным представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов производится уточнение персональных данных, соответствующая блокировка снимается.

5.5.6. В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с момента выявления, необходимо устранить

---

[3] В случае, если блокирование не нарушает права и законные интересы субъекта ПДн или третьих лиц.

[1] В случае, если в ИСПДн есть функционал, позволяющий осуществить блокирование персональных данных, работники Дирекции по информационным технологиям осуществляют блокирование внутренними средствами ИСПДн. Если указанный функционал отсутствует, работники Дирекции по работе с персоналом/подразделения, ответственного за обработку запроса субъекта ПДн, уведомляют причастных руководителей структурных подразделений Общества о необходимости блокирования персональных данных (временном прекращении обработки персональных данных в части запрета на передачу персональных данных в сторонние организации) соответствующего субъекта ПДн. Руководители структурных подразделений Общества, в свою очередь, оповещают причастных работников своих подразделений о блокировании данных.

допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий десяти рабочих дней с момента выявления неправомерности действий с персональными данными, необходимо уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Общество обязано уведомить субъекта ПДн или его законного представителя, а, в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

5.6 Уничтожение персональных данных

5.6.1. Персональные данные подлежат уничтожению, если иное не предусмотрено федеральными законами или соглашением между Обществом и субъектом ПДн, в следующих случаях:

- по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении;
- по требованию субъекта ПДн или уполномоченного органа по защите прав субъектов ПДн, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- выявления неправомерной обработки персональных данных и невозможностью устранения допущенных нарушений в срок, установленным законодательством Российской Федерации;
- отзыва субъектом ПДн согласия на обработку своих персональных данных.

5.6.2. В первом случае (по достижении цели обработки персональных данных или в случае утраты необходимости в их достижении) уничтожение персональных данных осуществляется в соответствии с регламентом, определяющим требования к формированию, учету, отбору, подготовки и передачи документов на архивное хранение и дальнейшего их использования.

5.6.3. В остальных трех случаях по результатам уничтожения персональных данных оформляется Акт (форма Акта приведена в Приложении 5).

5.6.4. Уничтожение персональных данных осуществляется только комиссией, состав комиссии утверждается приказом Генерального директора Общества:

- при уничтожении персональных данных, обрабатываемых в ИСПДн и материальных носителях, находящихся на площадках в городе Москве, в состав комиссии должны входить представители Юридической службы, Дирекции по информационным технологиям, структурного подразделения Общества, в чьем

ведении находятся указанные персональные данные и представителей Дирекции по информационным технологиям при необходимости.

- при уничтожении персональных данных, обрабатываемых в региональных подразделениях (филиалах) осуществляется силами работников филиалов, при этом состав комиссии должен быть сходным по своим функциональным обязанностям с приведенными.

5.6.5. Об устранении допущенных нарушений или об уничтожении персональных данных Общество обязано уведомить субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.6.6. В случае отзыва субъектом ПДн согласия на обработку своих персональных данных Общество обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Обществом и субъектом ПДн. Об уничтожении персональных данных Общество обязано уведомить субъекта ПДн.

6 Права и обязанности

6.1 Права субъектов ПДн

6.1.1. Субъект ПДн, персональные данные которого обрабатываются в Обществе, имеет право:

- получать доступ к своим персональным данным и ознакамливаться с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные (за исключением случаев, предусмотренных федеральным законом);
- получать от Общества:
  - подтверждение факта обработки персональных данных;
  - сведения о правовых основаниях и целях обработки персональных данных;
  - сведения о способах обработки персональных данных, применяемых Обществом;
  - сведения о наименовании и месте нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона;
  - перечень обрабатываемых персональных данных, относящихся к нему, и источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
  - сведения о сроках обработки персональных данных, в том числе сроках их хранения;
  - сведения о порядке осуществления субъектом ПДн прав, предусмотренных законодательством о персональных данных;
  - информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;
  - наименование и адрес лица, осуществляющего обработку персональных данных по поручению Общества;
  - сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его персональных данных;

- требовать от Общества уточнения, блокирования или уничтожения персональных данных, в случае если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленных целей обработки персональных данных;
- отозвать согласие на обработку своих персональных данных;
- обжаловать действия или бездействие Общества в установленном законом порядке, если субъект ПДн считает, что обработка его персональных данных осуществляется с нарушением требований Федерального закона № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы;
- принимать предусмотренные законом меры по защите своих прав и свобод;
- заявить возражение против порядка принятия решения на основании исключительно автоматизированной обработки Обществом персональных данных, а также получить разъяснения по порядку защиты своих прав и законных интересов.

6.2 Права и обязанности Общества в части обработки персональных данных

6.2.1. Общество обязано:

- обеспечить конфиденциальность персональных данных, то есть не допустить их распространения без согласия субъекта ПДн или наличия иного законного основания, за исключением случаев обезличенных персональных данных и в отношении общедоступных персональных данных;
- обеспечить безопасность персональных данных при их обработке в соответствии с требованиями законодательства Российской Федерации о персональных данных;
- обеспечить хранение первичной учетной документации по договорам страхования, учету труда и его оплаты, к которой, в частности, относятся документы по учету кадров, документы по учету использования рабочего времени и расчетов с работниками, по оплате труда и др. При этом персональные данные субъектов ПДн - работников не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные, при условии соблюдения сроков хранения, предусмотренных законодательством Российской Федерации;
- вести учет передачи персональных данных субъектов ПДн третьим лицам в соответствии с правилами делопроизводства, принятыми в Обществе;

- в случае реорганизации или ликвидации Общества осуществлять учет, сохранность и передачу персональных данных работников на государственное хранение в соответствии с законодательством Российской Федерации.

6.3 Ответственность

6.3.1. Лица, которым в силу трудовых отношений с Обществом стала известна информация, составляющая персональные данные, в случае нарушения режима защиты этих персональных данных несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами Российской Федерации.

Приложение №1

Форма Журнала однократного пропуска субъектов персональных данных на территорию Общества

Журнал
однократного пропуска субъектов персональных данных на территорию Общества

_____Наименование Общества_____

_____Место расположение Общества___

Ответственное лицо: _____
(фамилия, имя, отчество, должность лица (лиц),
ответственного за ведение журнала учета)

Подпись: _____

М.П.

№ п/п	Дата	Время	Фамилия, имя, отчество	Вид документа, с которым пропуск действителен	Куда (к кому) идет	Примечание

Приложение №2
Форма Журнала учета носителей информации, содержащей персональные данные

Экз. ед

ЖУРНАЛ

учета носителей персональных данных

№	Дата	Идентификатор и вид носителя		Ответственный за хранение	
				ФИО	Подпись
1	2	3		4	5

(продолжение таблицы)

Отметка о возврате (уничтожении)			Примечание
Номер и дата акта	ФИО	Подпись	
6	7	8	9

Приложение №3
Форма Журнала учета обращений субъектов персональных данных

Журнал

учета обращений граждан (субъектов персональных данных)

_____
(дата начала ведения Журнала)

_____Наименование Общества___

_____Место расположения Общества____

Ответственное лицо: _____
(фамилия, имя, отчество, должность лица (лиц),
ответственного за ведение журнала учета)

Подпись: _____
М.П.

№	Дата поступления (год, месяц, число)	Фамилия, имя, отчество подавшего обращение	Краткое содержание обращения	Кому и когда подано на исполнение	Срок исполнения	Когда и какое решение принято	Дело, в которое подшиты документы

Приложение №4

Форма Акта передачи документов (иных носителей), содержащих персональные данные

АКТ
приема-передачи документов (иных материальных носителей), содержащих персональные данные субъекта ПДн

На основании _____
_____ *(основание передачи персональных данных)* в лице _____
_____
___ *(Ф.И.О., должность работника, осуществляющего передачу персональных данных)* передает, а
_____
(*наименование Общества, принимающей документы (иные материальные носители), содержащие персональные данные*) в лице
_____
(*Ф.И.О., должность представителя Общества, принимающей документы (иные материальные носители), содержащие персональные данные субъекта персональных данных)* получает документы (иные материальные носители), содержащие персональные данные на срок ___ _____ и в целях:_____
_____
_____
(указать цель использования)

Перечень документов (иных материальных носителей), содержащих персональные данные субъекта персональных данных

№ п/п		Кол-во
Всего		

Полученные персональные данные могут быть использованы лишь в целях, для которых они сообщены. Незаконное использование предоставленных персональных данных путем их разглашения, уничтожения и другими способами, установленными федеральными законами, может повлечь соответствующую гражданско-правовую, материальную, дисциплинарную, административно-правовую и уголовную ответственность.

Передал _____ _____
(Ф.И.О., должность работника, осуществляющего передачу персональных данных) подпись

Принял _____ _____
(Ф.И.О., должность представителя Общества – приемщика документов (иных материальных носителей), содержащих персональные данные) подпись

Приложение №5
Форма Акта (Реестра) уничтожения информации, содержащей персональные данные

1. Форма Акта

УТВЕРЖДАЮ
Генеральный директор
_____
«___» _____ 20___ г.

АКТ № _____

об уничтожении персональных данных субъекта(ов) персональных данных
_____
(наименование Общества)

Мы, нижеподписавшиеся, _____
(должности, ф. и. о.)
_____
_____
_____

составили настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации (электронных, бумажных[5]) подлежат уничтожению.

Инвентарный номер (при наличии)	Причина уничтожения носителя информации; стирания информации	Тип носителя информации	Производимая операция (стирание, уничтожение)	Дата	Примечание
1	2	3	4	5	6

_____
(ф. и. о., подпись, дата)
_____
(ф. и. о., подпись, дата)
_____
(ф. и. о., подпись, дата)

Правильность произведенных записей в акте проверил _____
_____
(ф. и. о., подпись, дата)

Руководитель (ответственного подразделения) _____
_____
(ф. и. о., подпись, дата)

Регистрационные данные на носителях информации перед стиранием с них информации с записями в акте сверили, произвели стирание содержащейся на носителях информации.

_____

[5] В случае, если объем уничтожаемых документов позволяет перечислять их в Акте

(ф. и. о., подпись, дата)

_____

(ф. и. о., подпись, дата)

_____

(ф. и. о., подпись, дата)

Регистрационные данные на носителях информации (твердой копии) перед их уничтожением сверили с записями в акте и полностью уничтожили путем

_____

_____

(ф. и. о., подпись, дата)

_____

(ф. и. о., подпись, дата)

_____

(ф. и. о., подпись, дата)

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произвел:

Ответственный за учет _____

2. Уничтожение бумажных носителей (в случае их большого объема)

УТВЕРЖДАЮ
Генеральный директор
_____
«___» _____ 20___ г.

АКТ № _____

об уничтожении персональных данных субъекта(ов) персональных данных

_____
(наименование Общества)

Мы, нижеподписавшиеся, _____
(должности, ф. и. о.)
_____
_____
_____

составили настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации (твердая копия) подлежат уничтожению.

Дата уничтожения	Подразделение, в чьем ведении находятся уничтожаемые носители	Причина уничтожения носителя информации	Идентификационные данные (тип документов или период, за который уничтожаются носители…)	ФИО работника, проводившего уничтожение носителей	Примечание
1	2	3	4	5	6

_____
(ф. и. о., подпись, дата)
_____
(ф. и. о., подпись, дата)
_____
(ф. и. о., подпись, дата)

Правильность произведенных записей в акте проверил _____
_____
(ф. и. о., подпись, дата)

Руководитель (ответственного подразделения) _____
_____
(ф. и. о., подпись, дата)

Приложение №6
Требования к помещению для хранения персональных данных

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать средствами, препятствующими неконтролируемому проникновению в режимные помещения.

Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Режим охраны помещений, в том числе правила допуска сотрудников и в рабочее и нерабочее время, устанавливает Директор филиала по согласованию, при необходимости, установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются.

Двери спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе или у ответственного.

Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя. Дубликат ключа от хранилища ответственного пользователя в

опечатанной упаковке должен быть передан на хранение оператору под расписку в соответствующем журнале.

По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале ответственному пользователю или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает оператор или ответственный пользователь криптосредств.

В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств, ответственным пользователем криптосредств или оператором.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю криптосредств или оператору. Прибывший ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным пользователем криптосредств необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

Спецпомещения:

- Серверное помещение (хранение носителей персональных данных: резервные копии, флэш носители).
- Хранение договоров страхования (бумажный носитель персональных данных).
- Хранение материалов УУ (бумажный носитель персональных данных).
- Хранение ключевой информации (сейфы).