Приложение № 1
к Приказу АО «СК «Ю-Лайф»
от «21» сентября 2022 г. №339

ПОЛИТИКА
АКЦИОНЕРНОГО ОБЩЕСТВА «СТРАХОВАЯ КОМПАНИЯ «Ю-ЛАЙФ»
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2022 год

Общие положения

1.1. Настоящая «Политика Акционерного общества «Страховая компания «Ю-Лайф» в отношении обработки и защиты персональных данных» (далее – Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и является основополагающим внутренним документом АО «Страховая компания «Ю-Лайф» (далее – Компания), определяющим и регулирующим ключевые направления деятельности Компании в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Компания.

Настоящая Политика определяет цели, задачи и основные мероприятия по обеспечению безопасности ПДн в Компании от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Политика разработана в целях реализации требований законодательства РФ в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Компании, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Компанией как до, так и после утверждения Политики.

1.4. Политика раскрывает основные категории ПДн, обрабатываемых Компанией, цели, способы и принципы обработки Компанией ПДн, права и обязанности Компании при обработке ПДн, права субъектов ПДн, а также перечень мер, применяемых Компанией в целях защиты и обеспечения безопасности ПДн при их обработке.

1.5. Настоящая Политика распространяется на работников Компании, включая лиц, работающих по гражданско-правовым договорам, на работников сторонних организаций, взаимодействующих с Компанией на основании соответствующих нормативных, правовых и организационно-распорядительных документов, и лиц, действующих от имени Компании по поручению.

1.6. Настоящая Политика размещается на общедоступном ресурсе – на сайте Компании в сети Интернет по адресу: ”https://www.ulife.ru/”.

2. Источники нормативного правового регулирования вопросов обработки ПДн

2.1. Политика Компании в области обработки и защиты ПДн определяется в соответствии со следующими нормативными правовыми актами РФ:

- Трудовым кодексом Российской Федерации;
- Налоговым кодексом Российской Федерации;

- Федеральным законом № 152-ФЗ;

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Закон Российской Федерации от 27.11.1992 № 4015-1 «Об организации страхового дела в Российской Федерации»;

- Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»;

- Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении Требований к защите ПДн при их обработке в информационных системах ПДн»;

- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн»;

- Приказом ФСБ Российской Федерации № 378 от 10.07.2014 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите ПДн для каждого из уровней защищенности»

- другими нормативными документами уполномоченных органов.

2.2. Во исполнение настоящей Политики в Компании приказами руководителя утверждены локальные акты по вопросам обработки и защиты ПДн, в том числе определяющие для каждой цели обработки ПДн категории и перечень обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований.

2.3. Настоящая политика и иные локальные акты Компании не содержат положения, ограничивающие права субъектов ПДн, чьи ПДн обрабатываются в Компании, а также положения, возлагающие на Компанию не предусмотренные действующим законодательством Российской Федерации полномочия и обязанности.

3. Основные термины и понятия, используемые в локальных документах Компании, принимаемых по вопросу обработки ПДн

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн,

далее – Субъект ПДн).

Оператор – Акционерное общество «Страховая компания «Ю-Лайф», самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку ПДн, а также определяющее цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Информационная система ПДн (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Трансграничная передача ПДн – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Работники Компании – физические лица, состоящие с Компанией в трудовых отношениях на основании трудового договора или работающие по гражданско-правовым договорам.

Файлы cookie – файлы, установленные в компьютере, телефоне, планшете или любом другом техническом устройстве пользователя официального сайта Компании, для регистрации действий такого пользователя во время просмотра страниц официального сайта Компании. С помощью файлов cookie сервер, на котором находится официальный сайт Компании, распознает используемый пользователем браузер, предоставляя, например, зарегистрированному пользователю доступ к областям и сервисам без необходимости регистрации при каждом посещении и запоминая его предпочтения для будущих посещений.

Файлы cookie также используются для вычисления аудитории и параметров трафика, отслеживания прогресса и количества входов. Файлы cookie содержат данные в обезличенной форме.

4. Общие условия обработки Компанией ПДн

4.1. Обработка ПДн осуществляется в Компании на основе следующих принципов:

4.1.1. Обработка ПДн осуществляется на законной и справедливой основе.

4.1.2. Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

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

4.1.4. Обработке подлежат только ПДн, которые отвечают целям их обработки.

4.1.5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

4.1.6. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн.

4.1.7. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен соответствующим федеральным законом или иным нормативным правовым актом Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральными законами или иными нормативными правовыми актами Российской Федерации.

4.2. Обработка ПДн осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ.

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

4.2.2. Оператором осуществляется обработка специальной категории персональных данных - сведений о состоянии здоровья застрахованных лиц,

остальные данные из специальной категории касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни Оператором не обрабатываются.

5. Обработка ПДн

5.1. Получение ПДн.

5.1.1. ПДн получаются и обрабатываются Компанией на основании федеральных законов и иных нормативных правовых актов Российской Федерации, а в необходимых случаях – при наличии согласия субъекта ПДн.

5.1.2. Компания сообщает Субъекту ПДн о целях, предполагаемых источниках и способах получения ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа Субъекта дать согласие на их обработку, если такое согласие необходимо Компании в рамках заявленной цели.

5.1.3. Документы, содержащие ПДн, создаются путем:

- оформление, заключение, исполнение договоров страхования и иных гражданско-правовых договоров и сделок;
- оформления иных форм документов, необходимых для исполнения Компанией обязанностей, предусмотренных действующим законодательством Российской Федерации, в том числе в сфере противодействия легализации доходов, полученных преступным путем и финансирования терроризма;
- оформления документов, связанных с исполнением Компанией функций и обязанностей юридического лица в процессе своей деятельности;
- внесения сведений, полученных из оригиналов документов субъекта ПДн, в учетные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

5.2.4. Все ПДн Компания получает от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то Субъект уведомляется об этом или Компания у него получает согласие, за исключением следующих случаев:

- субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- ПДн получены Компанией на основании федерального закона и иного нормативного правого акта Российской Федерации или в связи с исполнением договора, стороной которого либо выгодоприобретателем по которому является субъект ПДн;
- ПДн данные разрешены субъектом ПДн для распространения или получены из общедоступного источника;

- уведомление субъекта ПДн нарушает права и законные интересы третьих лиц.

5.2.5. При сборе ПДн субъектов посредством информационно-телекоммуникационной сети Интернет Компания обеспечивает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, блокирование, удаление, уничтожение ПДн субъектов с использованием баз данных, находящихся на территории Российской Федерации.

Получение согласия субъекта на обработку ПДн осуществляется в случае предоставления субъектом любых личных данных с использованием электронных форм на сайте Компании.

Сайт Компании использует файлы «cookie» и собирает сведения о пользователях, в том числе с использованием стороннего сервиса «Яндекс.Метрика», которые необходимы Компании в целях анализа эффективности и улучшения работы сервисов сайта.

При посещении сайта Компания информирует пользователей о сборе и использовании файлов «cookie», а также об использовании сервиса «Яндекс.Метрика».

Дальнейшее использование сервисов сайта Оператора означает согласие субъекта персональных данных на обработку его файлов cookie в соответствии с условиями, определенными настоящей Политикой.

В случае отказа от обработки файлов cookie субъект персональных данных проинформирован о необходимости прекратить использование официального сайта Компании или отключить файлы cookie в настройках браузера. При этом субъект персональных данных также уведомлен и, соответственно, осознает, признает и соглашается с тем, что в таком случае отдельные разделы и (или) функции официального сайт Компании могут отображаться и (или) работать некорректно.

5.2. Обработка ПДн.

5.2.1. Обработка ПДн осуществляется:

- с согласия субъекта ПДн на обработку его ПДн;

- в случаях, когда обработка ПДн необходима для осуществления и выполнения возложенных на Компанию законодательством Российской Федерации и нормативными актами регуляторов, функций, полномочий и обязанностей;

- в случаях, когда осуществляется обработка ПДн, разрешенных субъектом ПДн для распространения.

5.2.2. Цели обработки ПДн:

• обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации (в том числе с целью осуществления и выполнения возложенных

законодательством Российской Федерации на оператора ПДн функций, полномочий и обязанностей;

- исполнение судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве);
- заключение и исполнение трудовых договоров с работниками (в том числе с целью содействия работникам в трудоустройстве, получении образования и продвижении по службе; обеспечения личной безопасности работников, контроля количества и качества выполняемой работы; обеспечения сохранности имущества; выплаты заработной платы и иных, причитающихся работникам, в соответствии с законодательством Российской Федерации или договором, выплат;
- осуществление предусмотренных законодательством Российской Федерации налоговых и социальных отчислений);
- ведение воинского учёта; организации постановки на индивидуальный (персонифицированный) учёт работников в системе обязательного пенсионного страхования;
- предоставление работникам дополнительных услуг за счёт оператора (в том числе с целью содействия работникам в оформлении зарплатной банковской карты и перечислении на неё заработной платы и иных, причитающихся работникам, в соответствии с законодательством Российской Федерации или договором, выплат;
- перечисление заработной платы и иных, причитающихся работникам, в соответствии с законодательством Российской Федерации или договором, выплат на иные банковские карты работников – в случае нежелания работников оформлять зарплатные банковские карты;
- содействие работникам и членам их семей в оформлении полиса добровольного медицинского страхования (ДМС);
- негосударственное пенсионное обеспечение, обеспечение командировок, оплата корпоративной телефонной связи или предложение оформления выгодных корпоративных тарифов у операторов телефонной связи и т.п.);
- предоставление работникам льгот и гарантий, предусмотренных законодательством Российской Федерации для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями);
- содействие в получении налоговых вычетов через оператора как работодателя;
- ведение кадрового делопроизводства; осуществление рекрутинга (привлечения и отбора кандидатов на работу), в том числе с целью предоставления кандидатам на работу возможности участия в отборе на замещение

соответствующих вакантных (открытых) должностей, содействия кандидатам, успешно прошедшим отбор на замещение соответствующих вакантных (открытых) должностей, в трудоустройстве;

- осуществление своей деятельности в соответствии с Уставом;
- предоставление субъектам ПДн доступа к официальному сайту оператора, размещённой на нём информации и имеющемуся функционалу;
- ведение статистики и отслеживание общего количества посетителей официального сайта оператора;
- улучшение официального сайта оператора и предоставление посетителям возможности индивидуально настраивать сервисы и функции официального сайта оператора;
- распознавание новых и старых пользователей официального сайта оператора;
- динамичное наблюдение за действиями пользователя и работой в браузерах при посещении официального сайта оператора;
- наилучшее понимание интересов посетителей официального сайта оператора;
- предоставление клиентам возможности регистрации (создания) учётной записи (личного кабинета) посредством имеющегося на официальном сайте оператора функционала; предоставление клиентам возможности получения доступа к своей учётной записи (личному кабинету) посредством прохождения процедур идентификации, аутентификации и авторизации, ознакомление с размещённой в такой учётной записи (личном кабинете) информацией и использование иного заранее предусмотренного и технически реализованного оператором функционала такой учётной записи (личного кабинета);
- хранение учётных данных (логинов и паролей, в том числе предыдущих) клиентов от созданных такими клиентами на официальном сайте оператора учётных записей (личных кабинетов клиентов);
- предоставление клиентам возможности изменения учётных данных (логинов и паролей) и (или) восстановления доступа к своей учётной записи (личному кабинету) на официальном сайте оператора (в случае утраты такого доступа) посредством смены пароля;
- обеспечение безопасности официального сайта оператора в целом и создаваемых клиентами на официальном сайте оператора учётных записей (личных кабинетов) от несанкционированного доступа в частности;
- осуществление гражданско-правовых отношений (в том числе с целью заключения, исполнения и прекращения гражданско-правовых договоров в случаях, предусмотренных законодательством Российской Федерации и Уставом оператора;

- выполнение возложенных на оператора функций, в том числе, но не ограничиваясь, организации, осуществляющей операции с денежными средствами в рамках Федерального закона от 07.08.2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» в объеме и на условиях предусмотренных законодательством РФ;
- заключение, исполнение договоров страхования и иных гражданско-правовых договоров и сделок;
- взаимодействие с лицом, намеренным заключить договор страхования;
- продвижение товаров (работ, услуг) оператора на рынке;
- оказание страховых услуг, контроль и оценка качества предоставляемых страховых услуг по всем вопросам их предоставления, предоставление сведений и информации по поводу и в связи с обращениями субъектов ПДн, а также в связи с возможными в дальнейшем требованиями/претензиями по таким обращениям, перестрахование рисков, принятых оператором по договорам страхования, и заключение, исполнение, изменение, прекращение соответствующих договоров перестрахования;
- урегулирование убытка в случаях обращения за выплатой страхового возмещения;
- получение и передача необходимой информации в единую автоматизированную систему, созданную в соответствии с Законом РФ от 27.11.1992 N 4015-1 «Об организации страхового дела в Российской Федерации»;
- осуществление и выполнение возложенных на оператора иными договорами прав и обязанностей, включая исполнение оператором договоров, стороной которых либо выгодоприобретателем или поручителем по которым является субъект ПДн;
- заключение договоров по инициативе субъекта ПДн или договоров, по которым субъект ПДн будет являться выгодоприобретателем или поручителем);
- ведение бухгалтерского учёта;
- заполнение и передача в органы исполнительной власти и иные уполномоченные организации требуемых форм отчётности;
- осуществление прав и законных интересов оператора и (или) третьих лиц;
- осуществление связи с субъектом ПДн в случае необходимости, в том числе с целью направления субъекту ПДн уведомлений, информации и запросов, связанных с деятельностью оператора, а также для обработки обращений (предложений, заявлений, заявок, запросов, жалоб, претензий и иных сообщений) субъектов ПДн;
- осуществление контрольно-пропускного режима, оказание

информационных услуг по сервисам и продуктам оператора;

- изготовление визитных карточек.

5.2.3. Категории субъектов ПДн:

- работники и бывшие работники;
- кандидаты для приема на работу (соискатели);
- родственники работников;
- страхователи, застрахованные лица, выгодоприобретатели, представители клиентов, агенты, представители контрагентов;
- кандидаты в члены совета директоров;
- акционеры;
- посетители сайта оператора и web-сервиса «Личный кабинет клиента».

5.2.4. ПДн, обрабатываемые Компанией:

Перечень ПДн, обрабатываемых в Компании, утверждается Приказом генерального директора Компании и по мере изменения состава обрабатываемых ПДн подлежит пересмотру и уточнению.

5.2.5. Обработка ПДн ведется:

- с использованием средств автоматизации, в том числе с передачей по сети Интернет по каналам связи, защищенным в соответствии с требованиями законодательства в области обеспечения безопасности информации;

- без использования средств автоматизации.

5.3. Хранение ПДн.

5.3.1. ПДн Субъектов ПДн могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

5.3.2. ПДн, зафиксированные на бумажных носителях хранятся в запираемых помещениях с ограниченным доступом.

5.3.3. ПДн Субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в машинных носителях информации, принадлежащих Компании.

5.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПДн.

5.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки. ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.4. Прекращение обработки ПДн

5.4.1. Обработка ПДн прекращается в следующих случаях:

- субъект ПДн потребовал немедленно прекратить обработку его ПДн, обрабатываемых в целях продвижения товаров, работ, услуг на рынке.

- выявлена неправомерная обработка ПДн, осуществляемая Компанией или лицом, действующим по поручению Компании;

- достигнута цель обработки ПДн;

- отзыв субъектом ПДн согласия на обработку его ПДн и в случае, если обработки ПДн более не требуется для выполнения обязанностей, возложенных на Компанию, или если иное не предусмотрено договором, стороной которого, выгодоприобретателем по которому является субъект ПДн, иным соглашением между Компанией и субъектом ПДн, либо если Компания не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации

5.5. Уничтожение ПДн.

5.5.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения). Для уничтожения бумажных документов допускается применение шредера.

5.5.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

5.5.3. Уничтожение документов (носителей), содержащих ПДн, производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

5.5.4. Уничтожение ПДн на электронных носителях сопровождается записями в журналах аудита программных средств, применяемых для уничтожения ПДн.

5.6. Передача ПДн.

5.6.1. Компанией осуществляется передача ПДн третьим лицам если она предусмотрена законодательством или если субъект выразил свое согласие на передачу. Во втором случае перечень лиц, которым передаются ПДн, указан в согласии на обработку ПДн, подписанном субъектом ПДн.

5.6.2. Оператор осуществляет трансграничную передачу ПДн клиентов в иностранных государствах, обеспечивающих адекватную защиту прав субъектов ПДн, в целях исполнения условий заключаемых договоров с перестраховщиками и сервисными компаниями с которыми у Оператора заключены договоры на оказание услуг. При этом трансграничная передача ПДн, относящихся к иным категориям субъектов ПДн, Оператором не осуществляется.

Оператор, при этом, обязуется предпринять все надлежащие действия для обеспечения конфиденциальности и безопасности любых ПДн, переданных на территорию любых иностранных государств.

5.6.3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого предполагается осуществлять передачу ПДн,

обеспечивается адекватная защита прав субъектов ПДн, до начала осуществления такой передачи.

5.6.4. Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта ПДн на трансграничную передачу его ПДн;
- исполнения договора, стороной которого является субъект ПДн.

5.7. Поручение обработки ПДн

5.7.1. Компания имеет право на поручение обработки ПДн третьим лицам в следующих случаях:

- субъект ПДн выразил свое согласие на поручение;
- поручение предусмотрено Российским или иным применимым законодательством в рамках установленной законодательством процедуры.

6. Принципы обеспечения безопасности ПДн

6.1. Основной задачей обеспечения безопасности ПДн при их обработке в Компании является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

6.2. Для обеспечения безопасности ПДн Компания руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Компании осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Компании и других имеющихся в Компании систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Компании с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем ПДн Компании, а также объема и состава обрабатываемых ПДн;

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Компании не дают возможности преодоления имеющихся в Компании систем защиты возможными нарушителями безопасности ПДн;

11) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

12) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация средств защиты ПДн осуществляются работниками, имеющими необходимые для этого квалификацию и опыт;

13) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Компании предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Компании до заключения договоров;

14) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн.

7. Доступ к обрабатываемым ПДн

7.1. Доступ к обрабатываемым в Компании ПДн имеют лица, уполномоченные приказом генерального директора Компании.

Перечень работников, допущенных к работе с ПДн, обрабатываемыми в Компании, разрабатывается и пересматривается по мере необходимости (изменение организационно-штатной структуры, введение новых должностей и т.п.).

7.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной функции закрепляются за соответствующими структурными подразделениями Компании.

7.3. Доступ работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних нормативных документов Компании.

Допущенные к обработке ПДн работники под подпись знакомятся с документами Компании, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных работников.

Работник Компании получает доступ к ПДн субъектов ПДн после:

- изучения и ознакомления под подпись с настоящей Политикой, Положением об обработке и защите ПДн и иными внутренними нормативными документами Компании, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных работников;
- прохождения инструктажа по информационной безопасности;
- ознакомления с видами ответственности за нарушение (невыполнение) норм законодательства РФ в сфере обработки ПДн.

7.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Компанией, определяется в соответствии с законодательством и внутренними нормативными документами Компании.

8. Реализуемые требования к защите ПДн

8.1. Компания принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.2. Состав указанных в пункте 8.1 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние нормативные документы об обработке и защите ПДн утверждаются (издаются) Компанией, исходя из требований:

- Федерального закона № 152-ФЗ;

- Трудового кодекса Российской Федерации;

- Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн»;

- Приказа ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн»;

- Постановления Правительства Российской Федерации от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»;

- Приказа ФСБ Российской Федерации № 378 от 10.07.2014 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите ПДн для каждого из уровней защищенности»;

- иных нормативных правовых актов Российской Федерации об обработке и защите ПДн.

8.3. В соответствии с требованиями нормативных документов в Компании создана система защиты ПДн (далее – СЗПДн), состоящая из подсистем правовой, организационной и технической защиты.

8.4. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПДн.

8.5. Подсистема организационной защиты включает в себя организацию структуры управления СЗПДн, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

8.6. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

8.7. Обеспечение безопасности ПДн в Компании при их обработке в ИСПДн достигается в Компании, в частности, путем:

1) определения угроз безопасности ПДн и оценки возможностей потенциальных нарушителей информационной безопасности. Тип актуальных угроз безопасности ПДн, оценка возможностей потенциальных нарушителей и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

2) определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности Компанией могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки средств защиты ПДн проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

3) применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

4) применения прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации средств криптографической защиты информации, когда применение таких средств необходимо для нейтрализации актуальных угроз;

5) проведения оценки эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

6) учета машинных носителей ПДн, обеспечение их сохранности;

7) обнаружения фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

8) восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним или воздействия внешних факторов;

9) установления правил доступа к обрабатываемым ПДн, а также обеспечения регистрации и учета действий, совершаемых с ПДн в ИСПДн;

10) установления индивидуальных паролей доступа работников в информационную систему в соответствии с их должностным обязанностями;

11) организации режима обеспечения безопасности помещений, в которых производится обработка ПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

12) осуществления контроля за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

8.8. Обеспечение защиты ПДн в Компании при их обработке, осуществляемой без использования средств автоматизации, достигается, в

частности, путем:

1) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

2) принятия мер по обеспечению раздельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

3) соблюдения требований:

- к раздельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;
- к уточнению ПДн;
- к уничтожению и обезличиванию;
- к использованию типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн;
- к хранению ПДн, в том числе к обеспечению раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

8.9. Для обеспечения защиты ПДн в Компании:

8.9.1. Назначено лицо, ответственное за организацию обработки ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением Компанией и его работниками требований к защите ПДн;

8.9.2. Разработаны документы, определяющие политику Компании в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, определяющие для каждой цели обработки ПДн категории и перечень обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Разработанные документы и локальные акты не содержат положения, ограничивающие права субъектов ПДн, а также возлагающие на Компанию не предусмотренные законодательством Российской Федерации полномочия и обязанности;

8.9.3. Разработана техническая документация на ИСПДн Компании, а также на систему защиты ПДн Компании;

8.9.4. Применяются средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия;

8.9.5. Соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ;

8.9.6. Осуществляется ознакомление работников, непосредственно задействованных в обработке ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними нормативным документами по вопросам обработки и защиты ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн;

8.9.7. Осуществляется внутренний контроль и аудит соответствия обработки ПДн Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике Компании в отношении обработки ПДн, локальным актам Компании;

8.9.8. Проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона № 152-ФЗ, определяется соотношение указанного вреда и принимаемых Компанией мер, направленных на обеспечение исполнения обязанностей, предусмотренных вышеуказанным Федеральным законом.

8.10. Перечень ПДн Компании утверждается Приказом генерального директора Компании.

8.11. Организация и проведение мероприятий по обеспечению защиты ПДн в Компании осуществляется в соответствии с Положением об обработке и защите ПДн, а также иными внутренними организационно-распорядительными и техническими документами Компании.

8.12. Общее руководство организацией работ по защите ПДн в Компании осуществляет генеральный директор Компании.

8.13. Деятельность Компании по обеспечению безопасности ПДн контролируется уполномоченным органом по защите прав субъектов ПДн.

9. Основные права субъекта ПДн и обязанности оператора

9.1. Основные права субъекта ПДн

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

9.1.2. Субъект ПДн имеет право на обращение к Компании и направлению ему запросов. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Компанией;

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

9.1.3. Порядок направления субъектами ПДн запросов на предоставление сведений об обработке ПДн определен требованиями Федерального закона № 152-ФЗ. В частности, в соответствии с указанными требованиями запрос на получение информации в Компанию должен содержать:

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

9.1.4. В случае направления запроса представителем субъекта ПДн, запрос должен содержать документ (копию документа), подтверждающий полномочия данного представителя.

9.1.5. Субъект ПДн имеет право на обжалование действий или бездействия Компании.

9.2. Обязанности Оператора

Оператор обязан:

- при сборе ПДн предоставить субъекту ПДн по его просьбе информацию о полученных ПДн;

- в случаях если ПДн были получены не от субъекта ПДн, уведомить субъекта ПДн, если субъект не был уведомлен соответствующим оператором;

- в случае отказа субъекта ПДн в предоставлении ПДн субъекту разъясняются юридические последствия такого отказа;

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;

- давать ответы на запросы и обращения Субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

9.3. Компания предпринимает необходимые и достаточные меры для поддержания точности и актуальности обрабатываемых ПДн, а также удаления ПДн в случаях, если они являются устаревшими, недостоверными или излишними, либо если достигнуты цели их обработки.

Субъекты ПДн несут ответственность за предоставление Компании достоверных сведений и документов, а также за своевременное обновление ПДн в случаях их изменений.

9.4. Иные права и обязанности субъектов и Компании ПДн определены положениями Федерального закона № 152-ФЗ и иными нормативными правовыми актами.