УТВЕРЖДАЮ

Генеральный Директор

Чумаченко М.В.

«28» июля 2015 г.

Положение об обработке и обеспечению безопасности персональных данных клиентов ООО «СК «Райффайзен Лайф»

Оглавление

1. Общие положения

1.1. Положением об обработке персональных данных в ООО «СК «Райффайзен Лайф» (далее – Положение и Организация соответственно) определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных клиентов-физических лиц Организации, являющихся страхователями, застрахованными лицами и выгодоприобретателями согласно договору страхования (индивидуальному и коллективному (групповому), (далее – клиент, субъект) в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 25 июля 2011 г. N 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119, Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иными нормативными актами, действующими на территории Российской Федерации.

1.2. В Положении используются следующие термины:

- **Безопасность персональных данных** – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн.
- **Блокирование персональных данных** – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).
- **Информационная система персональных данных** – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
- **Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.
- **Конфиденциальность персональных данных** – обязательное для соблюдения оператором (в данном случае Организацией) или иным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.
- **Неавтоматизированная обработка персональных данных** – обработка ПДн субъекта без использования средств вычислительной техники.

- **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.
- **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 ПДн.
- **Оператор (персональных данных)** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с персональными данными.
- **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).
- **Предоставление персональных данных** – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.
- **Распространение персональных данных** – действия, направленные на раскрытие ПДн неопределенному кругу лиц.
- **Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.
- **Трансграничная передача персональных данных** – передача ПДн на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
- **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

1.3. Упорядочение обращения с персональными данными имеет целью обеспечить защиту прав и свобод клиента при соблюдении законных прав и интересов Организации, а также контрагентов в связи со служебной необходимостью обработки, хранения, получения и передачи третьим лицам сведений, являющихся персональными данными клиента.

2. Область действия

2.1. Положение является обязательным для исполнения всеми работниками Организации, имеющими доступ к персональным данным.

3. Порядок получения персональных данных

3.1. В соответствии с пунктом 1 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» под персональными данными клиента понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3.2. Организация в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» является оператором, организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных клиентов при обработке уполномоченными лицами Организации и третьими лицами, осуществляющими обработку персональных данных клиентов по поручению Организации.

3.3. При получении и обработке персональных данных работники Организации, уполномоченные осуществлять обработку персональных данных, обязаны соблюдать следующие требования:

- обработка персональных данных клиентов осуществляется в целях выполнения требований договора страхования, по которому клиент является страхователем, застрахованным лицом или выгодоприобретателем, при обязательном условии соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, локальных нормативных документов Организации;
- работник Организации, принимающий ПДн субъекта, должен сообщить выбранным субъектом способом (устно или письменно) следующую информацию:
  - наименование, либо фамилия, имя, отчество и адрес Организации или его представителя;
  - цель обработки ПДн и ее правовое основание;
  - предполагаемые пользователи ПДн;
  - установленные действующим законодательством РФ права субъекта ПДн.
- запрещается получать и обрабатывать ПДн клиентов, не соответствующие целям их обработки;

- запрещается получать, обрабатывать и передавать третьим лицам установленные Федеральными законами от 27.07.2006 г. № 152-ФЗ «О персональных данных» специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной (частной) жизни, членстве в общественных объединениях, в том числе в профессиональных союзах как самого клиента, так и его ближайших родственников;
- при принятии решений, порождающих юридические последствия в отношении клиента или иным образом затрагивающих его права и законные интересы, запрещается основываться на персональных данных, полученных в результате исключительно автоматизированной обработки;
- защита персональных данных от неправомерного использования, разглашения, искажения и утраты обеспечивается за счет средств Организации в порядке, установленном Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119 и иными нормативными правовыми актами Российской Федерации;
- передача персональных данных клиента в пределах Организации осуществляется исключительно в соответствии с настоящим актом.
- передача персональных данных третьей стороне не допускается без письменного согласия клиента, за исключением случаев, установленных федеральными законами.

3.4. Обработка всех персональных данных должна производиться уполномоченными лицами Организации только с письменного согласия клиента. Письменное согласие клиента на обработку его ПДн должно включать в себя:

- фамилию, имя, отчество, адрес клиента, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя клиента, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты и приложенная нотариальная копия (или оригинал) доверенности или иного надлежащего документа, подтверждающего полномочия этого представителя (при получении согласия от представителя клиента);
- наименование и адрес Организации, получающего согласие клиента;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие клиента;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Организации, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Организацией способов обработки ПДн;
- срок, в течение которого действует согласие клиента, а также способ его отзыва, если иное не установлено действующим законодательством РФ;
- подпись клиента.

3.5. Обработка персональных данных клиентами уполномоченными лицами Организации и лицами, действующими по поручению Организации, возможна без их согласия в следующих случаях:

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов клиента, если получение согласия клиента невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов Организации или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы клиента;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен клиентом либо по его просьбе;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством РФ.

3.6. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн или в случае достижения целей обработки ПДн, Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, инициирует сбор, блокировку обработки с последующим уничтожением ПДн субъекта, кроме случаев, установленных законодательством РФ.

3.7. Письменные согласия субъектов передаются Работнику, ответственному за организацию обработки и обеспечение безопасности ПДн, и хранятся в специально предназначенном месте.

3.8. В случае получения запросов от уполномоченного органа по защите прав субъектов ПДн работник, ответственный за организацию обработки и обеспечение безопасности ПДн, обязан представить документы и локальные акты, по обеспечению безопасности обработки ПДн субъектов и (или) иным образом подтвердить принятие необходимых мер в течение тридцати дней с даты получения такого запроса.

4. Порядок обработки, передачи и хранения персональных данных

4.1. В соответствии с законодательством РФ в целях обеспечения прав и свобод человека и гражданина Организация и его представители при обработке ПДн клиента должны соблюдать следующие общие требования:

- обработка ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов РФ;
- при определении объема и содержания, обрабатываемых ПДн Организация должно руководствоваться действующим законодательством РФ и локальными нормативными актами Организации;
- при принятии решений, затрагивающих интересы клиента, Организация не имеет права основываться на ПДн клиента, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- защита ПДн клиента от неправомерного их использования или утраты обеспечивается Организацией в порядке, установленном действующим законодательством РФ;
- работники Организации должны быть ознакомлены под роспись с документами Организации, устанавливающими порядок обработки ПДн, а также об их правах и обязанностях в этой области;
- доступ Работников Организации к персональным данным субъектов ПДн в ИСПДн регламентируется только на основании локальных нормативных актов Организации с указанием перечня допущенных лиц, прав доступа, необходимых для выполнения служебных обязанностей;
- обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;
- уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление);
- уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными;

- при хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним;
- безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации;
- технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации, относящейся к персональным данным.

4.2. Реализация требований по обеспечению безопасности персональных данных в информационных системах возлагается на Управление информационных технологий Организации совместно со структурными подразделениями, обрабатывающими персональные данные. Перечень лиц, уполномоченных на обработку персональных данных, утверждается отдельным приказом.

4.3. Клиенты и их представители по их требованию должны быть ознакомлены с действующими документами Организации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

4.4. Право доступа к персональным данным клиентов имеют только специально уполномоченные лица, утвержденные приказом по Организации, при этом указанные лица должны иметь право получать только те персональные данные клиента, которые необходимы им для выполнения конкретных должностных функций.

4.5. В случае необходимости Организация вправе поручить обработку персональных данных другому лицу с согласия клиента данных, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Организации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством РФ, а также обязано выполнять требования защиты персональных данных, содержащиеся в поручении Организации.

4.6. Клиент, в установленном законодательством Российской Федерации и нормативными актами Организации порядке, имеет право:

- получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные;
- требовать от представителей Организации уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для работодателя персональных данных;
- своей волей и в своих интересах давать и отзывать согласие на обработку персональных данных для установленного локальными нормативными актами и федеральными законами круга лиц;

- требовать извещения представителями Организации всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия представителей Организации при обработке и защите его персональных данных.

4.7. Клиент, в установленном законодательством Российской Федерации и нормативными актами Организации порядке, имеет право получать от представителей Организации:

- подтверждение факта обработки ПДн в Организации;
- правовые основания и цели обработки ПДн;
- цели и применяемые в Организации способы обработки ПДн;
- наименование и место нахождения Организации, сведения о лицах (за исключением работников Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты ПДн на основании договора с Организацией 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 настоящим Федеральным законом;
- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Организации, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими Федеральными законами.

5. Обязанности Организации по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных

5.1. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя или уполномоченного органа по защите прав субъектов ПДн должно быть осуществлено блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечено их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) с момента такого обращения или получения указанного запроса на период внутренней проверки в Организации.

5.2. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн, должно быть осуществлено блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечено их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

5.3. В случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, должно быть проведено уточнение ПДн работником, ответственным за организацию обработки и обеспечение безопасности ПДн, либо обеспечено их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) в течение семи рабочих дней со дня представления таких сведений и снято блокирование ПДн. Уточнение ПДн должно производиться на основании данных, полученных от субъекта ПДн.

5.4. В случае выявления неправомерной обработки ПДн, осуществляемой Организацией или лицом, действующим по поручению Организации, Организация в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Организации. В случае, если обеспечить правомерность обработки ПДн невозможно, Организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Организация обязано уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

5.5. В случае достижения цели обработки ПДн Организация обязано прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) и уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Организацией и субъектом ПДн, либо если Организация не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законодательством.

5.6. В случае отзыва субъектом ПДн согласия на обработку его ПДн Организация обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Организацией и субъектом ПДн либо если Организация не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законодательством.

5.7. В случае невозможности уничтожения ПДн в течение срока, указанного в п. 5.4 – 5.6, Организация осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен Федеральными законами.

6. Мероприятия по защите персональных данных при их обработке и передаче в информационных системах персональных данных

6.1. В общем случае организационные мероприятия по защите ПДн связаны с формированием системы документов по защите ПДн, их разработкой, официальным оформлением и доведением до исполнителей, а также организацией контроля за соблюдением установленных этими документами правил и требований.

6.2. Мероприятия должны исключить возможность утечки информации, обрабатываемой в ИСПДн, и обеспечить запрет передачи ПДн по открытым каналам связи без применения установленных мер по ее защите, а также исключить возможность внесения в контролируемую зону устройств регистрации и накопления информации без соответствующего разрешения.

6.3. Мероприятия по защите ПДн, обрабатываемых на автоматизированном рабочем месте (далее – АРМ), должны быть связаны с обеспечением:

- сохранности машинных носителей информации, материалов печати и исключения доступа к ним посторонних лиц;
- ограничения физического доступа и контроль доступа к изменению конфигурации средств электронно-вычислительной техники (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.);
- минимизация возможностей несанкционированного просмотра изображений с монитора АРМ (терминала) через дверные проемы, окна – в том числе с использованием средств телевизионной, фотографической и визуальной оптической разведки, находящихся за границами контролируемой зоны;
- режима блокирования доступа к АРМ (терминалу) во время отсутствия Пользователя;
- режима блокирования доступа в помещение с установленным АРМ (терминалом) во внерабочее время и в рабочее время при отсутствии Пользователя.

6.4. Мероприятия по защите ПДн в локальных вычислительных сетях (далее – ЛВС) должны включать:

- обеспечение режима запрета на вхождение в сеть под чужой учетной записью;
- обеспечение периодической смены паролей Пользователями;
- обеспечение хранения файлов с информацией в групповых каталогах (каталогах, информация в которых является доступной для определенной группы лиц), структура которых однозначно отображает организационную структуру подразделения (управления, отдела, группы и др.) и разрешения доступа к нему только Работников соответствующей структурной единицы;
- обеспечение файлового обмена информацией между Пользователями подразделений через создаваемый каталог общего использования, информация в котором является доступной для имеющих санкционированный доступ в ЛВС Пользователей;
- обеспечение создания для каждого пользователя локальной вычислительной сети личного сетевого каталога, предназначенного для хранения пользовательских данных, и предоставление ему всех прав (чтение, запись, создание, удаление, переименование) в отношении информации указанного каталога, за исключением права изменения привилегий доступа;

- обеспечение контроля присвоения Пользователям учетных;
- обеспечение резервного копирования электронных информационных ресурсов;
- обеспечение режима разграничения и контроля доступа к аппаратным и программным ресурсам локальных вычислительных сетей и АРМ.

6.5. Технические мероприятия по защите информации разрабатываются по результатам обследования объекта информатизации, предназначенного для обработки ПДн, и оценки возможностей реализации замысла защиты на основе применения организационных мер защиты и активизации встроенных механизмов защиты используемых операционных систем и аппаратного обеспечения. Соответствующие требования излагаются в техническом задании на проектирование системы защиты.

7. Система документов по защите информации

7.1. Система документов по защите информации включает действующее законодательство РФ и локальные нормативные акты Организации.

7.2. Состав внутренних документов, разрабатываемых на основании действующего законодательства РФ и локальных нормативных актов Организации, определяется на этапе приведения процессов обработки ПДн в Организации в соответствие требованиям законодательства. Состав документов определяется Организацией при возможном привлечении организаций-лицензиатов.

7.3. В подразделении, обслуживающем ИСПДн, рекомендуется иметь комплект эксплуатационной и технической документации на ИСПДн, в том числе на систему защиты ПДн.

7.4. Обязанность поддерживать комплект документов по защите ПДн в актуальном состоянии возлагается на работника, ответственного за организацию обработки и обеспечение безопасности ПДн.

8. Контроль состояния системы защиты персональных данных

8.1. В рамках проверок состояния защиты ПДн рекомендуется осуществлять контроль:

- наличия в подразделениях нормативных документов по защите информации и доведения их до персонала с фиксацией факта ознакомления с документами;
- знания и выполнения работниками требований локальных нормативных актов Организации по защите ПДн при их обработке в ИСПДн Организации;
- наличия и комплектности эксплуатационной и технической документации на систему защиты ПДн, а также факта ознакомления работников Организации с инструкциями пользователей и администраторов средств защиты информации с соответствующей отметкой об ознакомлении в инструкциях;

- работоспособности системы защиты ПДн;
- задания требований по безопасности ПДн при разработке (модернизации) ИСПДн.

8.2. Контроль состояния защиты ПДн осуществляется в плановом и внеплановом порядке ответственным за организацию обработки и обеспечение безопасности ПДн Работником (либо комиссией), назначаемым Организацией.

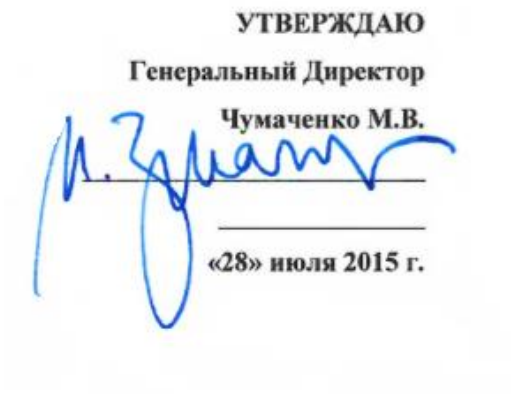
8.3. Результаты проверок оформляются в виде отчетов о проведении проверки.

9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

9.1. Работники Организации несут персональную ответственность за сохранность ПДн, к которым они имеют доступ.

9.2. Работники Организации, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, могут быть привлечены к ответственности, предусмотренной действующим законодательством РФ и локальными нормативными актами Организации.

Приложение 1



Образец письменного согласия на обработку
персональных данных клиента ООО «СК «Райффайзен Лайф»

(В согласие могут вноситься изменения, в частности, в зависимости от вида договора страхования (индивидуальный/коллективный) и от статуса клиента (страхователь, застрахованное лицо, выгодоприобретатель)

Согласие на обработку персональных данных
клиента ООО «СК «Райффайзен Лайф»
(страхователя, застрахованного лица и выгодоприобретателя
по договору страхования с ООО «СК «Райффайзен Лайф»)

Подписывая настоящее Заявление, я _____

- предоставляю Страховщику персональные данные и иную информацию обо мне, включающие, в том числе, помимо прочего: фамилию, имя, отчество; пол; год, месяц, дату и место рождения; место жительства (регистрации) и место пребывания; номер телефона; сведения о документе, удостоверяющем личность; ИНН; место работы, должность, профессию, служебные обязанности; сведения о состоянии здоровья (включая сведения, составляющие врачебную тайну), увлечениях (хобби); семейном, социальном и имущественном положении, содержащиеся в настоящем Заявлении, финансовой и

медицинской анкете, иных документах, заполняемых и подписываемых мною в связи с заключением и/или исполнением Договора страхования (далее - Персональные данные);

– своей волей и в своем интересе даю согласие Страховщику на автоматизированную, неавтоматизированную и смешанную обработку Персональных данных и любой информации обо мне (в том числе сведений, составляющих врачебную тайну), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование и уничтожение персональных данных и иной информации, сообщенной мной или моим представителем Страховщику в целях заключения и исполнения Договора страхования, осуществления страховых выплат и урегулирования страховых случаев, учёта Договора страхования в базах данных Страховщика и получения мной информации о продуктах и услугах Страховщика (далее - «Цели обработки»). Страховщик вправе в Целях обработки осуществлять трансграничную передачу Персональных данных и предоставлять Персональные данные (включая сведения, составляющие врачебную тайну) ЗАО «Райффайзенбанк», юридическим лицам, осуществляющим электронную обработку сведений о клиентах Страховщика, страховым агентам, страховым брокерам, перестраховочным организациям, моим представителям, аффилированным лицам Страховщика и лицам, входящим в группу лиц, в которую входит Страховщик, юридическим и финансовым консультантам, аудиторам Страховщика, а также иным лицам, если это необходимо для достижения Целей обработки и на основании соответствующих договоров, содержащих обязательство этих лиц по соблюдению конфиденциальности полученной информации;

согласен (согласна) с тем, что вышеизложенное согласие на обработку Персональных данных (включая сведения, составляющие врачебную тайну) действительно в течение пяти лет со дня подписания мною настоящего Заявления. В случае заключения Договора страхования между Страхователем и Страховщиком вышеизложенное согласие действует на весь период действия Договора страхования и в течение двадцати лет после прекращения всех обязательств сторон по вышеупомянутому Договору страхования. Я подтверждаю, что мне сообщено о порядке отзыва согласия на обработку моих персональных данных путем направления письменного заявления по месту нахождения Страховщика.