УТВЕРЖДЕНА
Приказом Генерального директора
Общества с ограниченной ответственностью
«Страховая компания «Мегарусс-Д»
от 18 сентября 2019 г. № 59-О/Д

Политика информационной безопасности информационных систем персональных данных ООО «СК «МЕГАРУСС-Д»

(редакция № 3)

Москва
2019 г.

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящая Политика информационной безопасности информационных систем персональных данных (далее – «Политика»), подготовленная в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – «Закон», 152-ФЗ), определяет позицию ООО «СК «Мегарусс-Д» (далее – «Общество», «Оператор») в области обработки и защиты персональных данных (далее – «ПДн»).

Настоящая Политика определяет принципы, порядок и условия обработки ПДн сотрудников Общества и иных лиц, чьи ПДн обрабатываются Обществом, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц Общества, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн.

Персональные данные являются конфиденциальной, строго охраняемой информацией и на них распространяются все требования, установленные внутренними документами Общества к защите конфиденциальной информации.

1.2. На основании приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от **21.06.2016 № 102** Общество включено в реестр операторов, осуществляющих обработку ПДн.

Регистрационный номер в реестре операторов, осуществляющих обработку ПДн: **77-16-004968**.

1.3. Настоящая Политика распространяется на ПДн, полученные как до, так и после ввода в действие настоящей Политики.

1.4. В настоящей Политике используются следующие термины:

Сотрудники – сотрудники ООО «СК «Мегарусс-Д».

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

Обработка персональных данных – 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.

Оператор – 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 ПДн.

Конфиденциальность персональных данных – обязательное для соблюдения Обществом или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Целостность персональных данных – состояние ПДн, при котором отсутствует любое их изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Доступность персональных данных – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Безопасность персональных данных – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в информационных системах.

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

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

2. Категории субъектов персональных данных и цели обработки персональных данных

2.1. Перечень ПДн, подлежащих защите в Обществе, формируется в соответствии с ФЗ РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

В зависимости от субъекта ПДн, Общество обрабатывает ПДн следующих категорий субъектов:

- ПДн сотрудника Общества - информация, необходимая Обществу в связи с трудовыми отношениями и касающиеся конкретного сотрудника;
- ПДн Клиента (потенциального Клиента, партнера, контрагента), а также персональные данные руководителя, участника (акционера) или сотрудника юридического лица, являющегося Клиентом (потенциальным Клиентом, партнером, контрагентом) Общества - информация, необходимая Обществу для выполнения своих обязательств в рамках договорных отношений с Клиентом и для выполнения требований законодательства Российской Федерации.

2.2. Общество осуществляет обработку ПДн в следующих целях:

- заключения, исполнения и прекращения гражданско-правовых договоров и договоров страхования с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством и Уставом Общества;
- организации кадрового учета Общества;
- обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам;
- ведения кадрового делопроизводства, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами;
- исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение;
- заполнения первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Уставом и внутренними документами Общества.

3. Правовые основания обработки персональных данных

3.1. Общество осуществляет обработку ПДн при наличии следующих правовых оснований:

* с согласия субъектов ПДн на обработку их ПДн;

* для исполнения договоров, стороной которых либо выгодоприобретателями или поручителями по которым являются субъекты ПДн, а также для заключения договоров по инициативе субъектов ПДн или договоров, по которым субъекты ПДн будет являться выгодоприобретателями или поручителями.

* для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных действующим законодательством Российской Федерации на Общество функций, полномочий и обязанностей.

Обработка ПДн в Обществе осуществляется в рамках следующих нормативно-правовых актов:

- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон 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»;
- Федеральный закон от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования»;
- Федеральный закон от 25.04.2002 № 40-ФЗ «Об обязательном страховании гражданской ответственности владельцев транспортных средств»;
- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в РФ»;
- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма»;
- Федеральный закон от 07.02.1992 № 2300-1 «О защите прав потребителей»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах»;
- Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Базовый состав организационных и технических мер»;
- Внутренний стандарт Всероссийского союза страховщиков «Обеспечение защиты конфиденциальной информации при осуществлении страховой деятельности» (утверждён постановлением Президиума Всероссийского союза страховщиков (протокол от 25.12. 2018 № 43).

4. Принципы обработки персональных данных

4.1. Общество при осуществлении своей деятельности осуществляет обработку ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение ПДн как с использованием средств автоматизации, так и без использования таких средств.

4.2. Обработка ПДн Обществом осуществляется на основе принципов:

- законности и справедливости целей и способов обработки ПДн;
- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Общества;
- соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих ПДн;
- хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки;
- уничтожения по достижении целей обработки ПДн или в случае утраты необходимости в их достижении.

5. Объем и категории обрабатываемых персональных данных. Условия обработки персональных данных

5.1. Перечень ПДн (в том числе специальных категорий ПДн), обрабатываемых в Обществе, определяется в соответствии с действующим законодательством Российской Федерации и внутренними нормативными документами Общества с учетом целей обработки ПДн, указанных в разделе 2, и в соответствии с Уведомлением об обработке ПДн, направленным Обществом в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

5.2. Обработка ПДн осуществляется в соответствии с заранее определенными и заявленными при сборе ПДн целями и задачами, а также полномочиями Общества, определенными действующим законодательством Российской Федерации, договорными отношениями с клиентами и контрагентами, Правилами и договорами страхования.

5.3. Получение и обработка ПДн в случаях, предусмотренных Законом о персональных данных, осуществляется с письменного согласия субъекта ПДн или при наличии иных оснований, установленных Законом о персональных данных. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и/или соглашением с клиентом.

5.4. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Обществом не осуществляется.

5.5. Обработка сведений о состоянии здоровья осуществляется в соответствии с Законом о персональных данных, Трудовым кодексом РФ, Федеральным законом «Об обязательном медицинском страховании в РФ».

5.6. Обработка сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), Обществом не осуществляется.

5.7. Право доступа к ПДн субъектов ПДн на бумажных и электронных носителях имеют только специально уполномоченные сотрудники Общества в пределах, установленных их должностными обязанностями.

5.8. Передача ПДн субъектов ПДн третьим лицам осуществляется в соответствии с требованиями действующего законодательства.

5.9. Общество вправе поручить обработку ПДн третьей стороне с согласия субъекта ПДн и в иных случаях, предусмотренных действующим законодательством Российской Федерации, на основании заключаемого с этой стороной договора (далее - Поручение). Третья сторона, осуществляющая обработку ПДн по Поручению Общества, обязана соблюдать принципы и правила обработки ПДн, предусмотренные Законом о персональных данных, обеспечивая конфиденциальность и безопасность ПДн при их обработке.

6. Права и обязанности

6.1. Права и обязанности Общества

Общество, как оператор персональных данных, вправе:

- отстаивать свои интересы в суде;
- предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении ПДн в случаях предусмотренных законодательством;
- использовать ПДн субъекта без его согласия, в случаях предусмотренных законодательством.

Компания, как оператор персональных данных, обязана обеспечить безопасность персональных данных.

6.2. Права и обязанности субъекта персональных данных

Субъект ПДн имеет право:

- требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

- требовать перечень своих ПДн, обрабатываемых Обществом, и источник их получения;
- получать информацию о сроках обработки своих ПДн, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке неправомерные действия или бездействия при обработке его ПДн;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Субъект персональных данных обязан:
- передавать Обществу комплекс достоверных, документированных ПДн, состав которых установлен законодательством;
- своевременно сообщать Обществу об изменении своих ПДн.

7. Обеспечение безопасности персональных данных. Требования по обеспечению безопасности персональных данных

7.1. При обработке ПДн Общество предпринимает необходимые организационные и технические меры для обеспечения безопасности ПДн от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

7.2. В целях координации действий по обеспечению безопасности ПДн в Обществе назначен Ответственный за организацию обработки ПДн, разработаны локальные акты по вопросам обработки ПДн.

7.3. Осуществляется периодическая оценка соответствия информационных систем ПДн требованиям законодательства и локальных актов по информационной безопасности.

7.4. Обеспечение безопасности ПДн достигается путём реализации следующих требований к защите ПДн:
- определением угроз безопасности ПДн при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей ПДн;
- установлением правил доступа к ПДн, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета действий, совершаемых с ПДн в информационной системе персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем персональных данных;

обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- выполнением всех иных требований к защите ПДн, установленных действующим законодательством Российской Федерации, в том числе, положениями Постановления Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8. Заключительные положения

Настоящая Политика является внутренним документом Общества, общедоступной и подлежит размещению на официальном сайте Общества.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите ПДн, но не реже одного раза в три года.

Контроль за исполнением требований настоящей Политики осуществляется ответственными за обеспечение безопасности ПДн в Обществе.

Ответственность должностных лиц Общества, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн, определяется в соответствии с законодательством Российской Федерации и внутренними документами Общества.