ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ФОНДА СОФПП (МКК)

1. Общие положения

1.1. Настоящая Политика (далее - Политика) определяет общие принципы и порядок обработки персональных данных (далее - ПДн) и меры по обеспечению их безопасности в Фонде СОФПП (МКК) (далее - Компания).

1.2. Целью Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, четкое и неукоснительное соблюдение требований законодательства Российской Федерации и международных договоров Российской Федерации в области ПДн.

1.3. Политика разработана с учетом требований Конституции Российской Федерации, в соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» (далее - Федеральный закон 152-ФЗ), Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», и другими федеральными законами, и подзаконными актами, определяющими случаи и особенности обработки ПДн.

1.4. В Политике используются следующие термины и определения:

– **автоматизированная обработка ПДн** - обработка ПДн с помощью средств вычислительной техники;

– **биометрические персональные данные** - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн;

– **блокирование ПДн** - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

– **дата-центр** - специализированная организация, предоставляющая услуги по размещению серверного и сетевого оборудования, сдаче серверов (в том числе виртуальных) в аренду, а также по подключению к сети Интернет;

– **доступ к персональным данным -** ознакомление определенных лиц (в том числе работников) с персональными данными субъектов, обрабатываемыми Компанией, при условии сохранения конфиденциальности этих сведений;

– **информационная система ПДн** - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

– **контрагент** - сторона договора с Компанией, не являющаяся работником Компании;

– **конфиденциальность ПДн** - обязанность лиц, получивших доступ к персональным данным, не раскрывать их третьим лицам и не распространять персональные данные без согласия субъекта ПДн, если иное не предусмотрено законодательством;

– **облачная вычислительная инфраструктура** - общий пул конфигурируемых вычислительных ресурсов (сети передачи данных, серверы, устройства хранения данных, приложения и сервисы - как вместе, так и по отдельности), к которым обеспечен повсеместной и удобный сетевой доступ по требованию, и которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру, обладающие пятью основными свойствами: самообслуживание по требованию; универсальный доступ по сети; объединение ресурсов; эластичность; учёт потребления;

– **обработка ПДн** - 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;

– о**бщедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен на основании законодательства субъектом ПДн либо по его просьбе или на основании его согласия, а также данные, которые подлежат обязательному раскрытию или опубликованию;

– **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, 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 персональными данными; в Политике под оператором понимается Компания, если иное не указано специально;

– **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн);

– **персональные данные, разрешенные субъектом ПДн для распространения**, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн путем дачи согласия на обработку ПДн, разрешенных субъектом ПДн для распространения в порядке, предусмотренном Федеральным законом «О персональных данных»;

– **предоставление ПДн** - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

– **распространение ПДн** - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

– **Роскомнадзор** - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, на которую возложены функции уполномоченного органа по защите прав субъектов ПДн, а также функции по федеральному государственному контролю (надзору) за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн;

– **специальные категории ПДн** - сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья;

– **субъект ПДн** - физическое лицо, к которому относятся персональные данные;

– **трансграничная передача ПДн -** передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

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

1.5. Субъект ПДн имеет право:

1.5.1. Получать информацию, касающеюся обработки его ПДн.

1.5.2. Требовать от Компании прекращения обработки своих ПДн, их уточнения блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также вправе принимать предусмотренные законодательством меры по защите своих прав;

1.5.3. В любой момент отозвать свое согласие на обработку ПДн;

1.6. Обязанности Компании:

1.6.1. Компания обязано предоставить субъекту ПДн или его представителю сведения, предусмотренные действующим законодательством.

1.6.2. В случае выявления неправомерной обработки ПДн Компания обязана осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн.

1.6.3. В случае предоставления субъектом ПДн или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются

необходимыми для заявленной цели обработки, Компания обязана уничтожить такие персональные данные и уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах, принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы

1.6.4. В случае выявления неправомерной обработки ПДн, осуществляемой Компанией или лицом, действующим по его поручению, Компания обязано прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Компании.

1.6.5. Компания проводит и документально оформляет в соответствии с требованиями, установленными Роскомнадзором, оценку вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона 152-ФЗ с целью соотнесения указанного вреда и принимаемых Компанией мер, направленных на обеспечение выполнения обязанностей, предусмотренных законом.

2. Правовые основания обработки ПДн

Порядок обработки и обеспечения безопасности ПДн регламентируют следующие законодательные и нормативные правовые акты Российской Федерации:

- Конституция Российской Федерации, принятая всенародным голосованием 12.12.1993;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;
- Гражданский кодекс РФ (часть первая) от 30.11.1994 № 51-ФЗ;
- Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ;
- Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ;
- Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ;
- Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ;
- Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете в Российской Федерации»;
- Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»;
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федеральный закон от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования»;
- Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
- Федеральный закон от 24.07.1998 № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»;
- Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;
- Федеральный закон от 26.02.1997 № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации»;

- Федеральный закон от 08.08.2001 № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей»;
- Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»;
- Постановление Госкомстата России от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах ПДн»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Приказ Минтруда России от 19.05.2021 № 320н «Об утверждении формы, порядка ведения и хранения трудовых книжек»;
- Договоры, заключаемые между Компанией и субъектом ПДн (контрагентами);
- Согласие субъектов ПДн на обработку их ПДн.

3. Принципы и цели обработки ПДн

Обработка ПДн Компанией осуществляется в соответствии со следующими принципами:

3.1. Законность и справедливая основа обработки ПДн. Компания принимает все необходимые меры по выполнению требований законодательства, не обрабатывает персональные данные в случаях, когда это не допускается законодательством и не требуется для достижения определенных Компанией целей, не использует персональные данные во вред субъектам таких данных.

3.2. Ограничение обработки ПДн достижением конкретных, заранее определённых и законных целей.

Целями обработки ПДн Компанией являются:

- **в отношении** Соискателей - подбор персонала (соискателей) на вакантные должности оператора;
- **в отношении Работников -** обеспечение соблюдения трудового законодательства; обеспечение соблюдения пенсионного законодательства РФ; обеспечение соблюдения законодательства РФ об обороне; ведение кадрового и бухгалтерского учета; обеспечение соблюдения страхового законодательства; обеспечение соблюдения законодательства РФ в сфере здравоохранения; обеспечение соблюдения законодательства РФ о безопасности; обеспечение соблюдения законодательства РФ о противодействии терроризму; обеспечение пропускного режима на территорию оператора; вознаграждение персонала; обеспечение соблюдения трудового

законодательства РФ в области охраны труда и благополучия сотрудников; обеспечение соблюдения законодательства РФ об исполнительном производстве; обеспечение соблюдения уголовно-исполнительного законодательства РФ; участие лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах; ннформационно-технологическое обеспечение деятельности; электронный документооборот;

– **в отношении Контрагентов и Представителей контрагентов** - оценка рисков при выборе контрагентов; ведение договорной работы с контрагентами; обеспечение соблюдения законодательства РФ об исполнительном производстве; обеспечение соблюдения уголовно-исполнительного законодательства РФ; участие лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

– **в отношении Посетители сайтов** - обработка пользовательских данных и администрирование сайтов Компании;

– **в отношении Плательщиков налога на профессиональный доход** - предоставление микрозаймов; поручительство; обработки заявок субъектов малого и среднего предпринимательства и граждан на предоставление поддержки; обработка запросов в онлайн-чате; проведения мероприятий по поддержке субъектов малого и среднего предпринимательства; передача отчетности;

– **в отношении Индивидуальных предпринимателей** - предоставление микрозаймов; поручительство; обработки заявок субъектов малого и среднего предпринимательства и граждан на предоставление поддержки; обработка запросов в онлайн-чате; проведения мероприятий по поддержке субъектов малого и среднего предпринимательства; передача отчетности;

– **в отношении Представителей юридических лиц** - предоставление микрозаймов; поручительство; обработки заявок субъектов малого и среднего предпринимательства и граждан на предоставление поддержки; обработка запросов в онлайн-чате; проведения мероприятий по поддержке субъектов малого и среднего предпринимательства; передача отчетности;

– **в отношении Спикеров** - проведения мероприятий по поддержке субъектов малого и среднего предпринимательства.

Описание целей обработки ПД, состава обрабатываемых ПД, категорий субъектов, ПД которых обрабатываются, правовых оснований такой обработки, а также сроках их обработки и хранения, способы обработки и действия изложены в Приложении №1 к настоящей Политике. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.3. Обработка только тех ПДн, которые отвечают заранее объявленным целям их обработки; соответствие содержания и объёма обрабатываемых ПДн заявленным целям обработки; недопущение обработки ПДн, не совместимой с целями сбора ПДн, а также избыточных по отношению к заявленным целям обработки ПДн. Компания не собирает и не обрабатывает персональные данные, не требующиеся для достижения целей, указанных в пункте 3.2 Политики, не использует персональные данные субъектов в каких-либо целях, кроме указанных.

3.4. Недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой.

3.5. Обеспечение точности, достаточности и актуальности ПДн по отношению к целям обработки ПДн. Компания принимает все разумные меры по поддержке актуальности обрабатываемых ПДн, включая (без ограничения) реализацию права каждого субъекта получать для ознакомления свои персональные данные и требовать от Компании их уточнения, блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленных выше целей обработки без объяснения причин такого требования.

3.6. Хранение ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен законодательством,

договором, стороной которого является субъект ПДн, а также согласием субъекта ПДн на обработку данных.

3.7. Уничтожение ПДн по достижении заявленных целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Компанией допущенных нарушений установленного законодательством порядка обработки ПДн, отзыве согласия на обработку субъектом ПДн, истечении срока обработки ПДн, установленных согласием на обработку ПДн, если иное не предусмотрено законодательством или договорами с субъектами ПДн.

4. Порядок и условия обработки ПДн

4.1. Компания осуществляет неавтоматизированную обработку ПДн; автоматизированную обработку ПДн с передачей полученной информации по информационно--телекоммуникационным сетям или без таковой; смешанную обработку ПДн.

4.2. Обработка ПДн может включать в себя, в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ, распространение), обезличивание, блокирование, удаление, уничтожение.

4.3. Обработка ПДн Компанией допускается в следующих случаях:

4.3.1. При наличии согласия субъекта ПДн на обработку его ПДн. Порядок получения Компанией согласия субъекта ПДн определен в разделе 6 Политики.

4.3.2. Обработка ПДн необходима для достижения целей, предусмотренных законом, а также для осуществления и выполнения возложенных законодательством на Компания функций, полномочий и обязанностей.

4.3.3. Для заключения договора по инициативе субъекта ПДн и исполнения договора, стороной которого является субъект ПДн.

4.3.4. Обработка ПДн Компанией необходима для осуществления прав и законных интересов Компании и/или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъектов ПДн.

4.3.5. Персональные данные подлежат опубликованию или обязательному раскрытию в соответствии с законодательством.

4.4. Компания не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта ПДн, если иное не предусмотрено законодательством, договором с субъектом ПДн, не указано в полученном от него согласии на обработку ПДн.

4.5. Органам власти, органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации персональные данные предоставляются (передаются) в соответствии с требованиями законодательства Российской Федерации.

4.6. Компания не обрабатывает персональные данные, относящиеся к специальным категориям и касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, о членстве субъектов ПДн в общественных объединениях или их профсоюзной деятельности, за исключением сведений, относящихся к вопросу о возможности выполнения Работником трудовой функции и необходимых для целей, определенных законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством, законодательством об обязательных видах страхования, со страховым законодательством.

4.7. Обработка ПДн о судимости может осуществляться Компанией исключительно в случаях и в порядке, установленных законодательством.

4.8. Компания не обрабатывает биометрические персональные данные.

4.9. При сборе ПДн Компания обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн с использованием баз данных,

находящихся на территории Компании и в дата-центрах на территории РФ.

4.10. Компания может не осуществлять трансграничную передачу ПДн. В случае необходимости передачи в иные страны такая передача осуществляется в соответствии с процедурой, установленной действующим законодательством.

5. Конфиденциальность ПДн

5.1. Работниками Компании, получившими доступ к персональным данным, должна быть обеспечена конфиденциальность таких данных.

5.2. Компания вправе с согласия субъекта поручить обработку ПДн другому лицу, если иное не предусмотрено законодательством, на основании заключаемого с этим лицом договора, предусматривающего в качестве существенного условия обязанность лица, осуществляющего обработку ПДн по поручению Компании, соблюдать принципы, правила обработки ПДн и требования к обработке, предусмотренные законодательством. Объем передаваемых другому лицу для обработки ПДн и количество используемых этим лицом способов обработки должны быть минимально необходимыми для выполнения им своих обязанностей перед Компанией.

В поручении Компании должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, перечень обрабатываемых по поручению ПДн, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, по запросу Компании в течение срока действия поручения, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных статьей 6 Федерального закона 152-ФЗ, должны быть указаны требования об уведомлении оператора о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, а также требования к защите обрабатываемых ПДн в соответствии со статьей 19 указанного закона.

При выполнении поручения Компании на обработку ПДн лицо, которому такая обработка поручена, вправе использовать для обработки ПДн свои информационные системы, соответствующие требованиям безопасности, установленным законодательством, что отражается Компанией в заключаемом договоре поручения на обработку ПДн.

5.3. Компания вправе разместить свои информационные системы ПДн в дата-центре (облачной вычислительной инфраструктуре). В этом случае в договор с дата-центром (провайдером облачных услуг) в качестве существенного условия может включаться требование о запрете доступа персонала дата-центра к информационным системам ПДн Компании, размещаемых в дата-центре (облачной инфраструктуре), и тогда такое размещение не рассматривается Компанией как поручение обработки ПДн дата-центру (провайдеру облачных услуг) и не требует согласия субъектов ПДн на такое размещение.

6. Согласие субъекта ПДн на обработку своих ПДн

6.1. Субъект ПДн принимает решение о предоставлении своих ПДн Компании и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, предметным, информированным, сознательным и однозначным и может предоставляться субъектом в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством.

6.2. Согласие Посетителя на обработку его ПДн дается в форме конклюдентных действий, а именно - предоставления документа, удостоверяющего личность, и сообщения сведений, запрашиваемых у него при посещении Компании.

6.3. Согласие Посетителей сайта на обработку их ПДн, получаемых Компанией при использовании файлов cookie, дается путем принятия условий «Политики в отношении файлов cookie» и простановки соответствующей отметки («галочки») в чек-боксе на сайте.

6.1. Согласие Плательщиков налога на профессиональный доход, Индивидуальных предпринимателей и Представителей юридических лиц на обработку их ПДн, получаемых Компанией при обращении в телефонном звонке, дается путем принятия условий об обработке ПДн при продолжении телефонного разговора.

6.2. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе является согласие в форме электронного документа, подписанного электронной подписью в соответствии с законодательством об электронной подписи.

6.3. Согласие субъектов на предоставление их ПДн не требуется при получении Компанией, в рамках установленных полномочий, мотивированных запросов от органов прокуратуры, правоохранительных органов, органов следствия и дознания, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства, и иных органов, уполномоченных запрашивать информацию в соответствии с компетенцией, предусмотренной законодательством.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

6.4. В случае поступления запросов от организаций, не обладающих соответствующими полномочиями, Компания предоставляет информацию только после получения согласия на предоставление его ПДн, и обязано предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что указанное правило будет (было) соблюдено.

7. Сведения о реализуемых требованиях к защите ПДн

7.1. Безопасность ПДн, обрабатываемых Компанией, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства в области защиты ПДн.

7.2. Правовые меры, принимаемые Компанией, включают:

– разработку локальных актов Компании, реализующих требования законодательства, в том числе - Политики и Положения о порядке обработки ПДн в Обществе;

– отказ от любых способов обработки ПДн, не соответствующих определенным в Политике целям и требованиям законодательства.

7.3. Организационные меры, принимаемые Компанией, включают:

– назначение лица, ответственного за организацию обработки ПДн;

– назначение лица, ответственного за обеспечение безопасности ПДн в информационных системах ПДн;

– ограничение состава работников Компании, имеющих доступ к персональным данным, и организацию разрешительной системы доступа к ним;

– ознакомление работников Компании, непосредственно осуществляющих обработку ПДн,

– положениями законодательства о ПДн, в том числе с требованиями к защите ПДн, с Политикой, другими локальными актами Компании по вопросам обработки ПДн;

– обучение всех категорий работников Компании, непосредственно осуществляющих обработку ПДн, правилам работы с ними и обеспечения безопасности обрабатываемых данных;

– определение в должностных инструкциях работников Компании обязанностей по обеспечению безопасности обработки ПДн и ответственности за нарушение установленного порядка;

– регламентацию процессов обработки ПДн;

– организацию учёта материальных носителей ПДн и их хранения, обеспечивающих предотвращение хищения, подмены, несанкционированного копирования и уничтожения;

– определение типа угроз безопасности ПДн, актуальных для информационных систем

ПДн, с учетом оценки возможного вреда субъектам ПДн, который может быть причинен в случае нарушения требований безопасности, определение уровня защищенности ПДн и требований к защите ПДн при их обработке в информационных системах, исполнение которых обеспечивает установленные уровни защищенности ПДн;

– определение угроз безопасности ПДн при их обработке в информационных системах, формирование на их основе частной модели (моделей) актуальных угроз;

– размещение технических средств обработки ПДн в пределах охраняемой территории;

– ограничение допуска посторонних лиц в помещения Компании, недопущение их нахождения в помещениях, где ведется работа с персональными данными и размещаются технические средства их обработки, без контроля со стороны работников Компании.

7.4. Технические меры, принимаемые Компанией, включают:

– разработку на основе модели актуальных угроз системы защиты ПДн для установленных Правительством Российской Федерации уровней защищенности ПДн при их обработке в информационных системах;

– использование для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия;

– оценку эффективности принимаемых мер по обеспечению безопасности ПДн;

– реализацию разрешительной системы доступа работников к персональным данным, обрабатываемым в информационных системах, и к программно-аппаратным и программным средствам защиты информации;

– регистрацию и учёт действий с персональными данными пользователей информационных систем, где обрабатываются персональные данные;

– ограничение программной среды;

– выявление вредоносного программного обеспечения (применение антивирусных программ) в узлах информационной сети Компании, обеспечивающих соответствующую техническую возможность;

– безопасное межсетевое взаимодействие (применение межсетевого экранирования);

– идентификацию и проверку подлинности пользователя (аутентификацию) при входе в информационную систему;

– контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;

– обнаружение вторжений в информационную систему Компании, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

– защита среды виртуализации;

– принятие мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы ПДн и по реагированию на компьютерные инциденты в них;

– защита сетевых устройств и каналов связи, по которым осуществляется передача ПДн;

– восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (создание системы резервного копирования и восстановления ПДн).

7.5. При размещении информационной системы в дата-центре (облачной инфраструктуре) часть мер безопасности может быть принята дата-центром (провайдером облачных услуг), что отражается в договоре между Компанией и дата-центром (провайдером облачных услуг).

8. Заключительные положения

8.1. Иные обязанности и права Компании как оператора ПДн и лица, организующего их обработку по поручению других операторов, определяются законодательством Российской Федерации в области ПДн.

8.2. Должностные лица и работники Компании, виновные в нарушении норм, регулирующих обработку и защиту ПДн, несут материальную, дисциплинарную, административную, гражданско- правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

8.3. Политика пересматривается по мере необходимости. Обязательный пересмотр Политики проводится в случае существенных изменений международного или законодательства Российской Федерации в сфере ПДн.

При внесении изменений в Политику учитываются:

– изменения в информационной инфраструктуре и (или) в используемых Компанией информационных технологиях;

– сложившаяся в Российской Федерации практика правоприменения законодательства в области ПДн;

– изменение условий и особенностей обработки ПДн Компанией в связи с внедрением в его деятельность новых информационных систем, процессов и технологий.