УТВЕРЖДЕНО
приказом Директора ООО «Мезекс. Информационные Системы»
№ ППД-2 от 01.06.2023

_____/Мезин Е.А./

ПОЛИТИКА ИНФОРМАЦИОННОЙ СИСТЕМЫ THEMEZEX.COM В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Пермь, 2023 год

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ 3
2. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 5
3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 5
4. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ 7
5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 9
6. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ 11
7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ 13
8. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ 18

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Политика Информационной системы TheMezEx.com в отношении обработки и защиты персональных данных (далее – «Политика») разработана во исполнение требований п.2 ч. 1 и ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Закон о персональных данных) в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2 Политика действует в отношении всех персональных данных, которые обрабатывает Оператор.

1.3 Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.4 Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на официальных сайтах Оператора.

1.5 Основные понятия, используемые в Политике:

1.5.1 **Оператор** и/или **ООО «Мезекс. Информационные Системы»** — Общество с ограниченной ответственностью «Мезекс. Информационные Системы», ОГРН 1225900009411, ИНН 5904401319, Юридический адрес 614010, Пермский край, г Пермь, ул Куйбышева, д. 95б, офис 1201/6.

1.5.2 **Субъект персональных данных** — физическое лицо, персональные данные которого обрабатываются Оператором на основании данного таким лицом согласия на обработку его персональных данных и настоящей Политики.

1.5.3 **Персональные данные** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (Субъекту персональных данных).

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

1.5.5 **Автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники.

1.5.6 **Распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.5.7 **Предоставление персональных данных** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.5.8 **Блокирование персональных данных** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

1.5.10 **Обезличивание персональных данных** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.5.11 **Информационная система персональных данных** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5.12 **Трансграничная передача персональных данных** — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.5.13 **Информационная система электронного взаимодействия TheMezEx.com** и/или **Информационная система TheMezEx.com** и/или **ИС** — программно-аппаратный комплекс,

включающий в себя приложение и сайт, на котором публикуются общие правила, условия договоров, оферты и соглашения, действующие между Участниками информационного обмена, а также системы автоматизированного формирования и отправки документов (через e-mail, telegram-bot-ы) и системы их акцепта и подписания.

1.5.14 **Клиент** — идентифицированное лицо с верифицированными данными, обращающееся в ИС с целью подбора способов удовлетворения своих потребностей.

1.5.15 **Участник ИС** — сертифицированное ИС лицо, на профессиональной основе осуществляющее деятельность по подбору способов удовлетворения потребностей Клиентов, с которыми последние обратились к ИС.

1.5.16 **Участники информационного обмена** — лица, обладающие доступом к сервису ИС по удаленному подписанию документов, а также лица, получившие в порядке Соглашения между участниками электронного взаимодействия информационной системы TheMezEx.com документы для подписания.

1.5.17 **Актуальные угрозы безопасности** — совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным в информационной системе Оператора, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия с персональными данными.

1.5.18 **Конфиденциальная информация** — информация, содержащая сведения конфиденциального характера, в том числе получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах, в отношении которой Оператор принимает меры по защите от несанкционированного доступа третьих лиц, не имеющих прав доступа к такой информации.

1.5.19 **Режим конфиденциальности** — правовые, организационные, технические и иные меры по защите Конфиденциальной информации, принимаемые ее обладателем.

1.5.20 **Реестр прав доступа** — локальный нормативный правовой акт Оператора, закрепляющий перечень и категории Конфиденциальной информации, ресурсы информационной системы Оператора, криптографические ключи, к которым имеют доступ лица, уполномоченные на обработку персональных данных.

1.6 Основные права и обязанности Оператора.

1.6.1 Оператор имеет право:

1) самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;

2) поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;

3) в случае отзыва Субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия Субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных.

1.6.2 Оператор обязан:

1) организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных и настоящей Политики;

2) отвечать на обращения и запросы Субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных и настоящей Политики;

3) сообщать в уполномоченный орган по защите прав Субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) по запросу этого органа необходимую информацию в течение 10 рабочих дней с даты получения такого запроса. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору необходимо направить в Роскомнадзор мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации;

4) в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование его о компьютерных инцидентах, которые повлекли неправомерную передачу (предоставление, распространение, доступ) персональных данных.

1.7 Основные права и обязанности Субъекта персональных данных:

1.7.1 Субъект персональных данных имеет право на:

1) получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются Субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим Субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;

2) требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3) выдвигать условие предварительного согласия при обработке персональных данных в целях продвижения на рынке товаров, работ и услуг;

4) обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

1.7.2 Субъект персональных данных обязан:

1) предоставлять Оператору полные и достоверные данные о себе;

2) в случае изменения сведений, составляющих персональные данные, не позднее пяти рабочих дней предоставить актуальную информацию Оператору.

1.8 Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, ответственным за организацию обработки персональных данных у Оператора.

1.9 Ответственность за нарушение требований законодательства Российской Федерации и локальных нормативных правовых актов Оператора в сфере обработки и защиты персональных данных определяется в соответствии с законодательством Российской Федерации.

2. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Правовым основанием обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, в том числе:

– Конституция Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Трудовой кодекс Российской Федерации;

– Налоговый кодекс Российской Федерации;

– Федеральный закон от 08.02.1998 № 14-ФЗ "Об обществах с ограниченной ответственностью"

– Федеральный закон от 06.12.2011 № 402-ФЗ "О бухгалтерском учете";

– Федеральный закон от 15.12.2001 № 167-ФЗ "Об обязательном пенсионном страховании в Российской Федерации";

– иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора.

2.2 Правовым основанием обработки персональных данных также являются:

– Устав Оператора;

– договоры, указанные в п. 3.3 Политики;

– согласия Субъектов персональных данных на обработку их персональных данных;

– локальные нормативные правовые акты Оператора, регулирующие отношения в области обработки персональных данных.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.2 Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

3.3 Обработка Оператором персональных данных осуществляется в следующих целях:

– передача персональных данных Клиента Участникам Информационной системы TheMezEx.com, а так же иным лицам, осуществляющим в рамках Информационной системы TheMezEx.com инвестиционную и иную деятельность по удовлетворению финансовых потребностей субъектов инвестирования, для принятия Клиентом оферт, а также для заключения Клиентом с ними и дальнейшего исполнения агентских договоров, агентских договоров на финансовый консалтинг, заключения и исполнения договоров купли-продажи, договоров предоставления займа (кредита), договоров уступки прав (требований), договоров залога, договоров аренды, договоров лизинга, договоров поручительства, договоров финансового консультирования и иных договоров, а также сопровождающих их документов, которые возможно будут заключены в целях удовлетворения финансовых потребностей Клиентов, за удовлетворением которых Клиент обратился в Информационную систему TheMezEx.com;

– передача персональных данных Клиента внутри Информационной системы TheMezEx.com для заключения между Клиентом и Участниками Информационной системы TheMezEx.com агентских договоров, агентских договоров на финансовый консалтинг для последующего удовлетворения финансовых потребностей Клиента путем принятия им оферт (соглашений, лицензионных договоров), а также заключения между Клиентом и лицами, осуществляющими в рамках Информационной системы TheMezEx.com инвестиционную и иную деятельность по удовлетворению финансовых потребностей субъектов инвестирования, договоров купли-продажи, договоров предоставления займа (кредита), договоров уступки прав (требований), договоров залога, договоров аренды, договоров лизинга, договоров поручительства, договоров финансового консультирования и иных договоров, а также любых сопровождающих их документов при их необходимости;

– верификация и идентификация Клиентов, Участников ИС и лиц, осуществляющих в рамках Информационной системы TheMezEx.com инвестиционную и иную деятельность по удовлетворению финансовых потребностей субъектов инвестирования, как сторон, заключающих сделки посредством Информационной системы TheMezEx.com, а также в целях реализации положений Соглашения между участниками электронного взаимодействия Информационной системы TheMezEx.com и иных локальных правовых актов, действующих в рамках Информационной системы TheMezEx.com;

– анализ и удовлетворение иных моих потребностей Клиентов за счет посреднической деятельности Участников ИС;

– получение Клиентами коммерческих предложений и/или иной информации о товарах, работах, услугах, их содержании, порядке их исполнения, выгодах, которые я (представляемое мной лицо) могу (может) получить от Оператора ПД, Участников Информационной системы TheMezEx.com, Субъектов инвестирования и иных лиц, осуществляющих в рамках Информационной системы TheMezEx.com инвестиционную и

иную деятельность по удовлетворению финансовых потребностей Субъектов инвестирования;

– осуществление проверки достоверности и полноты предоставленной Субъектом персональных данных информации;

– возникновение, осуществление, изменение и прекращение гражданских и иных правоотношений Субъекта персональных данных с Участниками Информационной системы TheMezEx.com и иными лицами, осуществляющими в рамках Информационной системы TheMezEx.com инвестиционную и иную деятельность по удовлетворению финансовых потребностей субъектов инвестирования, в том числе правоотношений в рамках гражданско-правовой и иной ответственности Субъекта персональных данных;

– обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;

– обеспечения нормального функционирования Информационной системы TheMezEx.com, касающегося процессов подписания договоров, которые возможно будут заключены для удовлетворения финансовых потребностей Клиента, с которыми он обратился в Информационную систему TheMezEx.com, а также процессов подбора Участников Информационной системы TheMezEx.com, лиц, осуществляющих в рамках Информационной системы TheMezEx.com инвестиционную и иную деятельность по удовлетворению финансовых потребностей субъектов инвестирования, и способов удовлетворения финансовых потребностей, с которыми Клиент обратился в Информационную систему TheMezEx.com;

– осуществление Оператором своей хозяйственной деятельности;

– ведение Оператором кадрового делопроизводства;

– содействие работникам Оператора в трудоустройстве, получении образования и продвижении по работе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества Оператора;

– привлечение и отбор кандидатов на работу у Оператора;

– организация постановки на индивидуальный (персонифицированный) учет работников в системе обязательного пенсионного страхования;

– заполнение и передача в органы исполнительной власти и иные уполномоченные организации требуемых форм отчетности;

– ведение Оператором бухгалтерского учета;

– улучшение работы официальных сайтов Оператора (сбор сведений об использовании сайтов, анализ посещаемости сайтов, проверка результативности).

3.4 Обработка персональных данных работников Оператора может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

4. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным разделом 3 настоящей Политики и согласием Субъекта персональных данных на обработку его персональных данных. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2 Оператор может обрабатывать персональные данные следующих категорий Субъектов персональных данных.

4.2.1 Кандидаты для приема на работу к Оператору:

– фамилия, имя, отчество;

– паспортные данные (дата рождения, место рождения, серия и номер паспорта, дата выдачи паспорта, наименование органа, выдавшего паспорт, код подразделения, адрес регистрации);

– место пребывания;

– адреса страниц в социальных сетях;

– номер телефона;
– сведения об образовании;
– сведения о последнем месте работы и причине увольнения.

4.2.2 Работники и бывшие работники Оператора:
– фамилия, имя, отчество;
– пол;
– гражданство;
– дата и место рождения;
– паспортные данные (дата рождения, место рождения, серия и номер паспорта, дата выдачи паспорта, наименование органа, выдавшего паспорт, код подразделения, адрес регистрации);
– адрес фактического проживания;
– контактные данные;
– индивидуальный номер налогоплательщика (ИНН);
– страховой номер индивидуального лицевого счета (СНИЛС);
– сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
– семейное положение, наличие детей, родственные связи;
– сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий;
– данные о регистрации брака;
– сведения о воинском учете;
– сведения об инвалидности;
– сведения об удержании алиментов;
– сведения о доходе с предыдущего места работы;
– иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

4.2.3 Члены семьи работников Оператора:
– фамилия, имя, отчество;
– степень родства;
– год рождения;
– иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

4.2.4 Участники ИС, Клиенты, лица, осуществляющие в рамках ИС инвестиционную и иную деятельность по удовлетворению финансовых потребностей субъектов инвестирования:
– фамилия имя отчество;
– пол;
– дата и место рождения;
– серия и номер паспорта;
– сведения об органе, выдавшем паспорт;
– дата выдачи паспорта;
– код подразделения;
– сведения о воинской обязанности;
– сведения о ранее выданных паспортах;
– адрес места жительства;
– адрес постоянной и временной регистрации;
– страховой номер индивидуального лицевого счёта (СНИЛС);
– индивидуальный номер налогоплательщика (ИНН);
– банковские реквизиты (наименование обслуживающего банка, расчетный счет, корреспондентский счет, номер банковской карты, иные банковские реквизиты);
– реквизиты временного удостоверения личности;
– реквизиты паспорта иностранного государства;
– реквизиты водительского удостоверения;
– реквизиты свидетельства о регистрации по месту пребывания;

– семейное положение;
– пол, фамилия имя отчество и личный код детей;
– социальное положение;
– сведения о профессиональной, трудовой и коммерческой деятельности;
– сведения об образовании;
– сведения о заработной плате и других доходах;
– сведения о размере произведенных налоговых отчислений;
– сведения о страховом пенсионном стаже, кредитной истории;
– размер индивидуального пенсионного капитала;
– сведения о контактных телефонах;
– адреса электронных почт;
– личные id мессенджеров;
– адреса страниц в социальных сетях;
– имущественное положение, сведения о принадлежащем Субъекту персональных данных движимом и недвижимом имуществе, включая информацию о залогах, арестах и иных ограничениях в отношении имущества, принадлежащего Субъекту персональных данных;
– сведения о выданных, действительных и отмененных доверенностях;
– сведения о проектах, в которых Субъект персональных данных является автором или исполнителем;
– сведения о финансовых потребностях Субъекта персональных данных;
– сведения о деловой репутации;
– сведения о наличии правонарушений, наличии задолженностей и долгов перед третьими лицами и публичными образованиями;
– сведения о ведущихся и завершенных, гражданских, административных и иных процессах;
– сведения о любых сертификатах и лицензиях, выданных Субъекту персональных данных, а так же их реквизиты;
– данные о лицах, аффилированных Субъекту персональных данных;
– данные о лицах, контролируемых Субъектом персональных данных;
– сведения, подтверждающие деловую репутацию Субъекта персональных данных;
– данные о принадлежащем аффилированным Субъекту персональных данных лицам движимом и недвижимом имуществе;
– фотографии, содержащие изображение лица Субъекта персональных данных;
– иные персональные данные, необходимые для возникновения, изменения, осуществления и прекращения гражданско-правовых и иных отношений в рамках целей, указанных в Политике.

4.2.5 Представители Участников ИС, Клиентов и лиц, осуществляющих в рамках ИС инвестиционную и иную деятельность по удовлетворению финансовых потребностей субъектов инвестирования:
– фамилия, имя, отчество;
– паспортные данные;
– контактные данные;
– замещаемая должность;
– фотографии, содержащие изображение лица Субъекта персональных данных;
– иные персональные данные, предоставляемые представителями Участников ИС, Клиентов и лиц, осуществляющих в рамках ИС инвестиционную и иную деятельность по удовлетворению финансовых потребностей субъектов инвестирования для возникновения, изменения, осуществления и прекращения гражданско-правовых и иных отношений в рамках целей, указанных в Политике.

4.3 Посетители официальных сайтов Оператора:
– тип, версия, язык операционной системы, браузера;
– тип устройства и разрешение экрана;
– страницы, открываемые посетителем сайта;
– MAC и IP-адреса;

– файлы cookies;
– иные данные в соответствии с условиями использования сервиса Яндекс.Метрика.
Вышеуказанные персональные данные посетителей сайтов Оператора обрабатываются Оператором с использованием интернет-сервиса веб-аналитики Яндекс.Метрика (ООО «ЯНДЕКС», 119021, Россия, Москва, ул. Л. Толстого, 16.). Сервис Яндекс.Метрика собирает обезличенную информацию о визитах посетителей сайтов. Сервис учитывает посетителей по анонимным идентификаторам браузеров, которые сохраняются в cookie. Собранную информацию сервис предоставляет Оператору путем составления отчетов об использовании сайтов, их посещаемости (конверсии). Полученные данные хранятся в Яндексе.
Оператор обрабатывает указанные обезличенные данные о посетителях Оператора в случае, если это разрешено в настройках браузера посетителя (включено сохранение файлов «cookie» и использование технологии JavaScript). Посетитель сайта может отказаться от использования cookies, выбрав соответствующие настройки в браузере.
4.4 Обработка Оператором биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) и специальных категорий персональных данных осуществляется в соответствии с законодательством Российской Федерации, согласием Субъекта персональных данных на обработку его персональных данных и настоящей Политикой.

5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.
5.2 Обработка персональных данных осуществляется с согласия Субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.
5.3 Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.
5.4 К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных, и иные лица, уполномоченные им на обработку персональных данных.
5.5 Обработка персональных данных осуществляется путем:
– получения персональных данных в устной и письменной форме непосредственно от Субъектов персональных данных;
– получения персональных данных в электронной форме через официальные сайты Оператора непосредственно от Субъектов персональных данных;
– получения персональных данных в письменной и электронной форме от Участников ИС;
– получения персональных данных из общедоступных источников;
– внесения персональных данных в журналы, реестры, ИС и иные информационные системы Оператора;
– использования иных способов обработки персональных данных.
5.6 Не допускается раскрытие третьим лицам и распространение персональных данных неограниченному кругу лиц без согласия на это Субъекта персональных данных, если иное не предусмотрено федеральным законом.
Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Требования к содержанию согласия на обработку персональных данных, разрешенных Субъектом персональных данных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 N 18.
5.7 Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

5.8 Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

– определяет угрозы безопасности персональных данных при их обработке;

– принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;

– назначает лиц, ответственных за обеспечение безопасности персональных данных в информационных системах Оператора;

– создает необходимые условия для работы с персональными данными;

– организует учет документов, содержащих персональные данные;

– организует работу с информационными системами Оператора, в которых обрабатываются персональные данные;

– хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

– организует обучение работников Оператора и иных лиц, осуществляющих обработку персональных данных.

5.9 Оператор осуществляет хранение персональных данных в форме, позволяющей определить Субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором или согласием на обработку персональных данных.

5.9.1 Персональные данные на бумажных носителях хранятся у Оператора в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации", Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 N 236)).

5.9.2 Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

5.10 Оператор прекращает обработку персональных данных в следующих случаях:

– выявлен факт их неправомерной обработки. Срок - в течение трех рабочих дней с даты выявления;

– достигнута цель их обработки;

– истек срок действия или отозвано согласие субъекта персональных данных на обработку указанных данных, когда по Закону о персональных данных обработка этих данных допускается только с согласия.

5.11 При достижении целей обработки персональных данных, а также в случае отзыва Субъектом персональных данных согласия на их обработку Оператор прекращает обработку этих данных, если:

– иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных;

– Оператор не вправе осуществлять обработку без согласия Субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

– иное не предусмотрено другим соглашением между Оператором и Субъектом персональных данных.

При обращении Субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных в срок, не превышающий 10 рабочих дней с даты получения Оператором соответствующего требования, обработка персональных данных прекращается, за исключением случаев, предусмотренных Законом о персональных данных. Указанный срок может быть продлен, но не более чем на пять

рабочих дней. Для этого Оператору необходимо направить Субъекту персональных данных мотивированное уведомление с указанием причин продления срока.
5.12 При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации исключительно с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

6. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

6.1 Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Оператором Субъекту персональных данных или его представителю в течение 10 рабочих дней с момента обращения либо получения запроса Субъекта персональных данных или его представителя. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору следует направить Субъекту персональных данных мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.
В предоставляемые сведения не включаются персональные данные, относящиеся к другим Субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.
Запрос должен содержать:
– номер основного документа, удостоверяющего личность Субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
– сведения, подтверждающие участие Субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;
– подпись субъекта персональных данных или его представителя.
Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
Оператор предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.
Если в обращении (запросе) Субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.
Право Субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Федерального закона о персональных данных, в том числе если доступ Субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.
6.2 В случае выявления неточных персональных данных при обращении Субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому Субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы Субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных Субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.3 В случае выявления неправомерной обработки персональных данных при обращении (запросе) Субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому Субъекту персональных данных, с момента такого обращения или получения запроса.

6.4 При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор:

– в течение 24 часов - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам Субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;

– в течение 72 часов - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

6.5 Порядок уничтожения персональных данных Оператором.

6.5.1 Условия и сроки уничтожения персональных данных Оператором:

– достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - в течение 30 дней;

– достижение максимальных сроков хранения документов, содержащих персональные данные - в течение 30 дней;

– предоставление Субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки - в течение семи рабочих дней;

– отзыв Субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

6.6 При достижении целей обработки персональных данных, а также в случае отзыва Субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

– иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных;

– Оператор не вправе осуществлять обработку без согласия Субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

– иное не предусмотрено другим соглашением между Оператором и Субъектом персональных данных.

6.7 Уничтожение персональных данных осуществляется комиссией, назначаемой приказом Оператора. Лицо, ответственное за уничтожение персональных данных, назначается председателем комиссии по уничтожению персональных данных.

6.8 При наступлении любого из событий, повлекших необходимость уничтожения персональных данных, в соответствии с законодательством Российской Федерации, лицо, ответственное за уничтожение персональных данных обязано:

– уведомить членов комиссии о работах по уничтожению персональных данных;

– определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);

– установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);
– определить технологию (приём, способ) уничтожения персональных данных (и/или материальных носителей персональных данных);
– определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение персональных данных;
– руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных);
– оформить соответствующий акт об уничтожении персональных данных (и/или материальных носителей персональных данных) и представить акт об уничтожении персональных данных (и/или материальных носителей персональных данных) на утверждение Оператору;
– в случае необходимости уведомить об уничтожении персональных данных Субъекта персональных данных и/или уполномоченный орган.

7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. На информацию, содержащую персональные данные, распространяется Режим конфиденциальности.
7.2. Организация работы по защите персональных данных.
7.2.1. Безопасность персональных данных при их использовании и обработке Оператором обеспечивается с помощью системы защиты Конфиденциальной информации, разработанной Оператором (далее — Система защиты).

При разработке Системы защиты учитывалась обязанность Оператора обеспечивать защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, в том числе принимать меры, установленные статьей 19 Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных».
7.2.2. Система защиты реализуется путем проведения нескольких взаимосвязанных процессов. К ним относятся:
– определение Актуальных угроз безопасности персональных данных;
– определение необходимых правовых, организационных и технических мер по обеспечению безопасности персональных данных, при их обработке в информационных системах Оператора, исполнение которых обеспечивает необходимый уровень защищенности;
– надлежащее применение определенных правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах Оператора, а также применение прошедших в установленном порядке процедуру оценки соответствия средств защиты персональных данных;
– проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных с установленной в настоящей Политике периодичностью;
– обеспечение контроля надлежащей реализации мер по обеспечению безопасности персональных данных.
7.2.3. В целях обеспечения функционирования Системы защиты Оператор выполняет следующие функции:
– организация разработки проектов и утверждение внутренних документов Оператора по вопросам обеспечения Режима конфиденциальности, определения режима и порядка обращения с персональными данными;
– организация взаимодействия с органами государственной власти, правоохранительными и надзорными органами по вопросам обеспечения и соблюдения Режима конфиденциальности;
– утверждение Реестра прав доступа, в том числе при внесении изменений и дополнений;

– определение требований к техническому оснащению помещений, в которых осуществляется работа с персональными данными;
– осуществление контроля за обеспечением режима безопасности помещений;
– принятие решений о необходимости проведения обучений лиц, ответственных за обработку персональных данных;
– проведение плановых и внезапных проверок на предмет соблюдения Режима конфиденциальности персональных данных;
– принятие решений о необходимости отстранения от взаимодействия с Конфиденциальной информацией лиц, нарушающих Режим конфиденциальности персональных данных;
– рассмотрение иных вопросов обеспечения и соблюдения Режима конфиденциальности.
7.2.4. Защите подлежат все персональные данные, определенные разделе 4 настоящей Политики.
7.3. Правовые меры защиты персональных данных.
7.3.1. К правовым мерам защиты персональных данных относятся:
1) Разработка и утверждение Оператором локальных нормативных актов, которыми регламентируется порядок организации Системы защиты;
2) Обязанность Оператора осуществлять мониторинг действующего законодательства.
7.3.2. Регламентирующие документы должны пересматриваться на предмет их актуальности и необходимости внесения изменений не реже одного раза в год, а также:
– в случае изменения законодательства, регламентирующего порядок обращения с Конфиденциальной информацией и устанавливающего требования к защите информации, в том числе законодательства о персональных данных;
– в случае установления фактов несанкционированного доступа к персональным данным, грубого нарушения Режима конфиденциальности, разглашения и утечки информации, содержащей персональные данные;
– на основании заключения, сформированного по результатам проведения очередной оценки достаточности принятых мер по защите персональных данных.
7.4. Организационные меры защиты персональных данных.
К организационным мерам защиты персональных данных относятся:
7.4.1. Определение правил доступа к информации, содержащей персональные данные.
7.4.1.1. К работе с информацией, содержащей персональные данные, могут быть допущены лица при одновременном выполнении следующих условий:
– лицо указано в Реестре прав доступа;
– лицо ознакомлено под роспись с настоящей Политикой;
– лицом подписано обязательство о неразглашении Конфиденциальной информации.
7.4.1.2. Приказом Оператора с целью определения перечня лиц, доступ которых к информации, содержащей персональные данные, необходим для выполнения ими своих обязанностей, и определения необходимого объема информации, содержащей персональные данные, утверждается Реестр прав доступа.
1) При утверждении Реестра прав доступа Оператор руководствуется правилом о том, что доступ к персональным данным должен предоставляться только тем лицам, которым персональные данные необходимы для выполнения возложенных на них функций и только в том объеме (к той ее части), который необходим для выполнения ими определенных функций.
2) Реестр прав доступа содержит следующую информацию:
– лица, допущенные к работе с информацией, содержащей персональные данные;
– категории информации, к которым лица, допущенные к обработке персональных данных, имеют доступ;
– ресурсы информационной системы Оператора, к которым лица, допущенные к обработке персональных данных, имеют доступ;

– Криптографические ключи, к которым имеют доступ лица, допущенные к обработке персональных данных.

3) Реестр прав доступа подлежит обязательному пересмотру не реже одного раза в год, а также в случае:

– изменения перечня лиц, допущенных к обработке персональных данных;
– изменения функционала лиц, допущенных к обработке персональных данных;
– изменения перечня ресурсов информационной системы Оператора;
– приобретения или уничтожения Криптографических ключей.

4) Правом предоставления, ограничения, прекращения доступа ко всей информации, содержащей персональные данные, создаваемой, хранимой и обрабатываемой в информационной системе Оператора, включая информацию, полученную от третьих лиц, обладает Оператор.

7.4.1.3. До начала работы с персональными данными лицо, которому планируется предоставить право обработки персональных данных, должно подписать обязательство о неразглашении Конфиденциальной информации.

7.4.1.4. Определение обязанностей для лиц, допущенных к работе с персональными данными.

Лицо, допущенное к работе с информацией, содержащей персональные данные, обязано:

– знать и выполнять требования настоящей Политики, иных внутренних документов Оператора по защите информации;
– соблюдать ограничения, установленные Реестром прав доступа: работать только с теми сведениями и использовать только те ресурсы информационной системы Оператора, которые определены Реестром прав доступа;
– соблюдать порядок работы и меры по защите ставших ему известными сведений конфиденциального характера;
– соблюдать правила работы с носителями информации, содержащей персональные данные, порядок их учета и хранения, обеспечивать в процессе работы сохранность сведений, содержащихся в них, от посторонних лиц;
– незамедлительно в письменной форме информировать Оператора о попытках несанкционированного доступа к информационным ресурсам и сведениям, содержащим персональные данные, о попытках подкупа, угроз, шантажа другими лицами с целью получения доступа к указанной информации;
– давать письменные объяснения о допущенных личных нарушениях установленного порядка работы, учета и хранения документов, содержащих персональные данные, и машинных съемных носителей информации, а также о фактах их утраты, передачи другим лицам.

7.4.1.5. Определение ограничений для лиц, допущенных к обработке персональных данных.

Лицу, допущенному к работе с информацией, содержащей персональные данные, запрещается:

– передавать сведения конфиденциального характера и документы (в устной форме, по телефону, на бумажных и машинных носителях, в электронной виде и т.д.) посторонним лицам;
– использовать информацию, содержащую персональные данные, в открытой переписке, статьях и выступлениях, а также в личных интересах;
– сообщать (обсуждать) по телефону сведения, содержащие персональные данные;
– копировать и хранить документы, содержащие персональные данные, на личных машинных съемных носителях информации;
– выполнять работы с материальными и машинными носителями, содержащими персональные данные, вне помещений, предназначенных для работы с персональными данными;
– выносить из помещений, предназначенных для работы с персональными данными, документы и машинные носители с информацией, содержащей персональные данные.

7.4.2. Назначение лица, ответственного за информационную безопасность.

Приказом Оператора назначается лицо, ответственное за информационную безопасность. В число его обязанностей входят:

– организация процесса реализации норм, установленных настоящей Политикой, в том числе обеспечение работы Системы защиты информации, содержащей персональные данные;

– обеспечение применения в информационной системе Оператора определенных мер защиты информации, содержащей персональные данные;

– контроль за соблюдением лицами, допущенными к обработке персональных данных, требований настоящей Политики;

– проведение обучений лиц, допущенных к обработке персональных данных, в целях ознакомления с требованиями настоящей Политики;

– сбор и анализ статистических данных об Актуальных угрозах безопасности, характерных для информационной системы Оператора;

– внесение предложений Оператору о необходимости проведения оценки достаточности принятых мер по защите информации, содержащей персональные данные, предложений по внесению изменений во внутренние документы Оператора, регламентирующие деятельность Оператора по защите информации, содержащей персональные данные, предложений по иным вопросам, связанным с деятельностью Оператора по защите информации, содержащей персональные данные.

7.4.3. Определение порядка передачи персональных данных.

7.4.3.1. При передаче персональных данных Оператор должен соблюдать следующие требования:

– не сообщать персональные данные третьей стороне без согласия Субъекта персональных данных за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта персональных данных, а также в случаях, установленных законодательством Российской Федерации;

– предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они получены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

– передавать персональные данные Субъекта персональных данных представителям Субъекта персональных данных в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций;

7.4.4. Обеспечение сохранности материальных носителей информации.

7.4.4.1. Режим сохранности материальных носителей информации.

1) Доступ к материальным носителям информации, содержащей персональные данные, имеют только лица, допущенные к обработке персональных данных.

2) Доступ к материальным носителям информации, содержащей персональные данные, посторонним лицам запрещен.

3) Рабочие места лиц, допущенных к обработке персональных данных, размещаются таким образом, чтобы исключить возможность обозрения находящихся на столе документов, а также мониторов компьютеров посторонними лицами.

4) Материальные носители, содержащие персональные данные, должны храниться в специальных сейфах или запирающихся металлических шкафах.

5) Персональные данные, обработка которых осуществляется в различных целях, хранятся раздельно.

7.4.4.2. Режим сохранности машинных носителей информации.

1) Учет машинных носителей информации осуществляется лицом, ответственным за информационную безопасность, путем ведения журнала учета машинных носителей информации. В журнале учета машинных носителей информации каждый машинный носитель информации закрепляется за ответственным лицом, допущенным к работе с персональными данными, который не вправе передавать закрепленный за ним машинный носитель информации третьим лицам.

2) Запрещается копирование файлов с информацией, содержащей персональные данные, и хранение их на жестких дисках рабочих станций (компьютеров, ноутбуков), съемных машинных носителях информации, других устройствах, способных накапливать и хранить информацию в электронном виде, за исключением случаев, описанных в настоящей Политике.

3) Оператор приобретает съемные машинные носители информации, способные накапливать и хранить информацию, для использования лицами, допущенными к обработке персональных данных. Такие машинные носители должны проверяться на наличие вирусов и вредоносных программ на регулярной основе.

7.4.5. Установление режима использования Криптографических ключей.

7.4.5.1. Оператор осуществляет учет Криптографических ключей путем закрепления права их использования за определенным лицом в Реестре прав доступа. При этом каждый Криптографический ключ используется только Оператором или лицом, допущенным к работе с персональными данными и включенным в Реестре прав доступа.

7.4.5.2. Передача Криптографических ключей, в случае если Криптографический ключ размещен на материальном носителе, не допустима.

7.4.5.3. Криптографические ключи должны эксплуатироваться их пользователями в соответствии с технической документацией.

7.4.6. Установление режима обеспечения безопасности помещений.

7.4.6.1. В целях исключения возможности неконтролируемого проникновения или пребывания посторонних лиц в помещениях, в которых обрабатывается и (или) хранится информация, содержащая персональные данные, Оператор устанавливает режим обеспечения безопасности этих помещений.

7.4.6.2. Требования к помещениям, в которых обрабатывается и (или) хранится информация, содержащая персональные данные, а также правила доступа к таким помещениям устанавливаются в локальном нормативном акте по обеспечению безопасности помещений, который утверждается Оператором.

7.4.7. Обнаружение фактов несанкционированного доступа к персональным данным, а также фактов нарушения лицами, допущенными к обработке персональных данных, Режима конфиденциальности.

7.4.7.1. Оператор принимает меры по обнаружению фактов несанкционированного доступа путем:

– установления обязанности лиц, допущенных к обработке персональных данных, сообщать о фактах, свидетельствующих о несанкционированном доступе к информации, содержащей персональные данные, в том числе о фактах несанкционированного проникновения в помещения, в которых обрабатывается и(или) хранится информация, содержащая персональные данные;

– применения технических средств обнаружения фактов несанкционированного доступа к помещениям, в которых обрабатывается и (или) хранится информация, содержащая персональные данные.

7.4.7.2. Каждый факт несанкционированного доступа фиксируется лицом, ответственным за информационную безопасность.

7.4.7.3. По всем фактам нарушений лицами, допущенными к обработке персональных данных, Режима конфиденциальности должны быть проведены расследования, в ходе которых необходимо определить круг лиц, виновных в этих нарушениях и причастных к ним, а также причины и условия, способствовавшие совершению данных нарушений. К проведению расследования привлекается лицо, ответственное за информационную безопасность.

7.4.7.4. По каждому факту несанкционированного доступа к персональным данным, а также факту нарушения лицами, допущенными к обработке персональных данных, Режима конфиденциальности проводится анализ причин и условий, способствовавших совершению указанных фактов, по результатам которого составляется заключение, содержащее дополнительные меры и предложения по защите персональных данных, а также план по реализации данных мер, включающий сроки их реализации и ответственных лиц.

7.5. Технические меры по защите персональных данных:
7.5.1. Приобретение и установка антивирусного программного обеспечения. Обязательным условием для приобретения антивирусного программного обеспечения является наличие лицензии. Антивирусное программное обеспечение должно регулярно обновляться в соответствии с последней версией. Антивирусное программное обеспечение устанавливается на все персональные компьютеры лиц, допущенных к обработке персональных данных.
7.5.2. Создание учетных записей для лиц, допущенных к обработке персональных данных. Каждому пользователю, обрабатывающему информацию, содержащую персональные данные, присваиваются личная учетная запись, для входа в которую устанавливается пароль. Пароль для входа в учетную запись не может совпадать с паролем для входа в учетные записи иных лиц, допущенных к обработке персональных данных. Пароль для входа в учетную запись не может передаваться третьим лицам, за исключением случаев, установленных настоящей Политикой.
7.5.3. Установление режима защиты сетевого взаимодействия. Обмен данными между элементами информационной системы Оператора и другими компьютерами (рабочими станциями, серверами) должен быть организован через защищенные соединения, организованные с использованием протоколов IPSec с проверкой подлинности и шифрованием IP-пакетов.
7.5.4. Осуществление резервного копирования информации, содержащей персональные данные.
7.5.5. Ограничение доступа к информационно-коммуникационной сети Интернет для лиц, допущенных к обработке персональных данных.
7.5.6. Учетным записям пользователей, допущенных к обработке персональных данных, может быть ограничен доступ к сети Интернет и средствам электронной почты.
7.5.7. Применение технических средств, обеспечивающих восстановление модифицированной или уничтоженной вследствие несанкционированного доступа информации, содержащей персональные данные.
7.6. Проведение оценки эффективности принятых мер по защите информации, содержащей персональные данные.
7.6.1. Оценка эффективности принятых мер по защите информации, содержащей персональные данные, может проводиться Оператором самостоятельно или с привлечением сторонней организации.
7.6.2. Оценка эффективности принятых мер по защите информации, содержащей персональные данные, проводится по результатам внутренней проверки, проводимой лицом, ответственным за информационную безопасность.
7.6.3. Приказом Оператора утверждаются периодичность проведения проверок выполнения условий настоящей Политики (но не реже одного раза в год), сроки проведения плановых проверок, а также их содержание.
7.6.4. По результатам проведения проверок составляется письменный отчет, который должен содержать:
– сведения обо всех фактах несанкционированного доступа к информации, содержащей персональные данные, нарушения лицами, допущенными к обработке персональных данных, Режима конфиденциальности;
– предложения по внесению изменений в Систему защиты информации, содержащей персональные данные, и сведения о достаточности принятых мер по защите информации, содержащей персональные данные.
7.6.5. В случае подтверждения недостаточности принятых мер по защите информации, содержащей персональные данные, Оператор принимает решение о необходимости применения дополнительных мер по изменению Системы защиты информации, содержащей персональные данные, в целях приведения ее к достаточному уровню.
7.7. Контроль за соблюдением лицами, допущенными к обработке персональных данных, требований, предъявляемых к ним и установленных настоящей Политикой, осуществляется лицом, ответственным за информационную безопасность.

8. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

8. Лица, виновные в нарушении порядка обращения с персональными данными, несут предусмотренную законодательством Российской Федерации ответственность.

8.1. Дисциплинарная ответственность:

a) Разглашение персональных данных Субъекта персональных данных, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих персональные данные Субъекта персональных данных; иные нарушения обязанностей по их защите, обработке и хранению, установленных настоящей Политикой, а также иными локальными нормативными актами Оператора, лицом, ответственным за получение, обработку и защиту персональных данных Субъекта персональных данных, влекут наложение на него дисциплинарного взыскания – выговора, увольнения (пп. «в» п.6 ч. 1 ст. 81 Трудового кодекса РФ).

b) В случае причинения ущерба Оператору лицо, имеющее доступ к персональным данным Субъектов персональных данных и совершившее указанный дисциплинарный поступок, несет полную материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 Трудового кодекса РФ.

8.2. Административная ответственность:

a) За нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП РФ).

b) За разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

8.3. Уголовная — за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили ущерб правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения.