

**ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ПЛАНЕТА»**

УТВЕРЖДЕНО
Приказ от «01» сентября 2025 г. № 4/пд

**Политика общества с ограниченной ответственностью «ПЛАНЕТА»
в отношении обработки персональных данных**

1. Общие положения

1.1. Положение об обработке и защите персональных данных (далее - Положение) издано и применяется в ООО «ПЛАНЕТА» (далее - Оператор, Организация) в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Настоящее Положение определяет цели, порядок и условия обработки персональных данных, категории субъектов, персональные данные которых обрабатываются, категории, перечень обрабатываемых персональных данных, способы, сроки их обработки и хранения, порядок уничтожения таких данных при достижении целей обработки или при наступлении иных законных оснований, устанавливает процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, связанных с обработкой и защитой персональных данных.

Все вопросы, связанные с обработкой и защитой персональных данных, не урегулированные настоящим Положением, разрешаются в соответствии с действующим законодательством Российской Федерации в области персональных данных.

1.2. К субъектам, персональные данные которых обрабатываются в Организации в соответствии с Положением, относятся:

- 1.2.1. Кандидаты для приема на работу в Организацию.
- 1.2.2. Работники Организации.
- 1.2.3. Бывшие работники Организации.
- 1.2.4. Члены семей работников Организации - в случаях, когда согласно законодательству сведения о них предоставляются работником.
- 1.2.5 Пациенты Организации.

1.3. Цели обработки персональных данных и категории (перечни) обрабатываемых персональных данных.

1.3.1. Персональные данные субъектов, перечисленных в пп. 1.2.1 - 1.2.4, обрабатываются с целью применения и исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ними отношений, в том числе:

- при содействии в трудоустройстве;
- ведении кадрового и бухгалтерского учета;
- содействии работникам в получении образования и продвижении по службе;
- оформлении наград и поощрений;
- предоставлении со стороны Организации установленных законодательством условий труда, гарантий и компенсаций;
- заполнении и передаче в уполномоченные органы требуемых форм отчетности;

- обеспечении личной безопасности работников и сохранности имущества;
- осуществлении контроля за количеством и качеством выполняемой работы.

1.3.2. В соответствии с целью, указанной в п. 1.3.1 Положения, в Организации обрабатываются следующие персональные данные:

- фамилия, имя, отчество (при наличии), а также прежние фамилия, имя, отчество (при наличии), дата и место их изменения (в случае изменения);
- пол;
- дата (число, месяц, год) и место рождения;
- фотографическое изображение;
- сведения о гражданстве;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении);
- сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);
- сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы;
- сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории Российской Федерации (для иностранных граждан, прибывающих в Российскую Федерацию);
- сведения, содержащиеся в разрешении на временное проживание, разрешении на временное проживание в целях получения образования (для иностранных граждан, временно проживающих в Российской Федерации), виде на жительство (для иностранных граждан, постоянно проживающих в Российской Федерации);
- сведения о доходах, обязательствах по исполнительным документам;
- банковский счет;
- сведения о состоянии здоровья (медицинских работников);
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (для работников, оказывающих услуги несовершеннолетним);
- иные персональные данные, содержащиеся в документах, представление которых предусмотрено законодательством, если обработка этих данных соответствует цели обработки, предусмотренной п. 1.3 Положения;
- иные персональные данные, которые работник пожелал сообщить о себе, и обработка которых соответствует цели обработки, предусмотренной п. 1.3 Положения.

1.3.3. Персональные данные субъектов, перечисленных в пп. 1.2.5, обрабатываются с целью

применения и исполнения законодательства в сфере здравоохранения в рамках исполнения договора об оказании Организацией медицинских услуг пациенту.

1.3.4. В соответствии с целью, указанной в п. 1.3.3 Положения, в Организации обрабатываются следующие персональные данные:

- фамилия, имя, отчество (при наличии);
- пол;
- дата (число, месяц, год) и место рождения;
- фотографическое изображение;
- сведения о гражданстве;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- сведения о состоянии здоровья;
- иные персональные данные, содержащиеся в документах, представление которых предусмотрено законодательством, если обработка этих данных соответствует цели обработки, предусмотренной п. 1.3.3 Положения.

1.3.5. Организация не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством Российской Федерации.

1.4. Действие настоящего Положения не распространяется на отношения, возникающие:

1) при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных фондов в соответствии с законодательством об архивном деле в Российской Федерации;

2) при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.5. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и настоящим Положением.

Обработка организована Оператором на принципах:

- законности целей и способов обработки персональных данных, добросовестности и справедливости в деятельности Оператора;
- ограничения обработки персональных данных достижением конкретных, заранее

определенных и законных целей;

- достоверности персональных данных, их достаточности для целей обработки;
- обработки только персональных данных, которые отвечают целям их обработки. Недопустима обработка персональных данных, несовместимая с целями сбора персональных данных;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обеспечения точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных. Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;
- хранения 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, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

1.6. Настоящее Положение и изменения к нему утверждаются приказом руководителя Оператора.

1.7. Работники Оператора, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены под подпись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными нормативными актами по вопросам обработки персональных данных, с данным Положением и изменениями к нему. Обучение указанных работников организуется структурным подразделением по повышению квалификации в соответствии с утвержденными Оператором графиками.

1.8. При обработке персональных данных Оператор применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.9. Режим конфиденциальности персональных данных Оператор обеспечивает в соответствии с настоящим Положением.

1.10. Контроль за соблюдением работниками Оператора требований законодательства Российской Федерации и положений локальных актов Оператора организован в соответствии с Положением о внутреннем контроле Оператора при обработке персональных данных. Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

1.11. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Оператором требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», осуществляется в соответствии с Требованиями, утвержденными Приказом Роскомнадзора от 27.10.2022 № 178.

Оценка вреда заключается в определении степени вреда, который может быть причинен субъекту персональных данных, в зависимости от характера персональных данных и видов их обработки.

Результаты оценки вреда оформляются актом оценки вреда.

1.12. Опубликование или обеспечение иным образом неограниченного доступа к настоящему Положению, иным документам, определяющим политику Оператора в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных Оператор проводит в соответствии с настоящим Положением.

1.13. Настоящее Положение и сведения о реализуемых требованиях к защите персональных данных должны быть опубликованы на сайте Оператора <https://www.palitra-pitania.ru/>. Оператор обязан обеспечить доступ к сайту и опубликованным сведениям.

1.14. Хранение персональных данных осуществляется в порядке, предусмотренном настоящим Положением.

1.15. Взаимодействие с федеральными органами исполнительной власти по вопросам обработки и защиты персональных данных субъектов, персональные данные которых обрабатываются Оператором, осуществляется в рамках законодательства Российской Федерации.

2. Порядок обеспечения Оператором прав субъекта персональных данных

2.1. Субъекты персональных данных или их представители обладают правами, предусмотренными Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими нормативно-правовыми актами, регламентирующими обработку персональных данных.

2.2. Оператор обеспечивает права субъектов персональных данных в порядке, установленном гл. 3 и 4 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.3. Полномочия представителя на представление интересов каждого субъекта персональных данных подтверждаются доверенностью, оформленной в соответствии со ст. ст. 185 и 185.1 Гражданского кодекса Российской Федерации или удостоверенной нотариально согласно ст. 59 Основ законодательства Российской Федерации о нотариате (утв. Верховным Советом Российской Федерации 11.02.1993 № 4462-1).

2.4. Сведения, указанные в ч. 7 ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», предоставляются субъекту персональных данных Ответственным ОПД в доступной форме без персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

2.5. Сведения, указанные в ч. 7 ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», предоставляются субъекту персональных данных или его представителю

Ответственным ОПД в течение 10 (десяти) рабочих дней с момента обращения либо получения Оператором запроса субъекта персональных данных или его представителя.

Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. 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), 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 Федерального закона от 27.07.2006 № 152-ФЗ «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.

2.6. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

2.7. Обработка персональных данных в целях продвижения медицинских услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных. Согласие может быть устным или письменным.

2.7.1. Индивидуальное устное общение с потенциальными потребителями производится по специально выделенной телефонной линии Оператора. При этом рабочее место работника Оператора, которому поручено общение, обеспечивается техническими средствами, позволяющими в автоматизированном режиме вести регистрацию телефонных вызовов, а также (с согласия субъекта персональных данных) вести аудиозапись переговоров. В данной ситуации аудиозапись полученного устного согласия является надлежащей.

2.7.2. Для письменного согласия достаточно простой письменной формы.

2.8. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в п. 2.7 Положения.

2.9. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами Российской Федерации, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

2.10. Оператор обязан устно, а по письменному требованию субъекта персональных данных или его представителя - письменно разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

2.11. Оператор обязан рассмотреть возражение, указанное в п. 2.10 настоящего Положения, в течение 30 (тридцати) дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

2.12. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных, а также с информацией, касающейся обработки его персональных данных, по месту своего расположения в рабочее время.

2.13. Оператор обязан уведомить субъекта и его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3. Порядок и условия обработки персональных данных

3.1. Организация до начала обработки персональных данных обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных ч. 2 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.2. В зависимости от целей обработки персональных данных Оператор использует следующие способы сбора персональных данных:

- получение оригиналов документов либо их копий;
- копирование оригиналов документов;
- внесение сведений в учетные формы на бумажных и электронных носителях;
- создание документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесение персональных данных в информационные системы персональных данных.

3.3. Условия обработки персональных данных Оператором:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных законодательством Российской Федерации, в том числе в сфере здравоохранения, трудового права, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта

персональных данных невозможно.

3.4. Обработка персональных данных осуществляется как без использования, так и с использованием средств автоматизации.

В Организации используются следующие информационные системы:

- автоматизированная система управления персоналом: имеются стандартные конфигурации 1С ЗУП на отдельном рабочем компьютере, не имеющим доступа к остальной инфраструктуре.
- корпоративная электронная почта: из почты на корпоративном домене используется только palitrainfo@yandex.ru, её хостинг осуществляется со стороны компании Яндекс. Собственной почтовой инфраструктуры в Организации нет;
- информационный портал: отсутствует;
- система электронного документооборота: не внедрена;
- система нормативно-справочной информации: отсутствует;
- система поддержки рабочего места пользователя: не внедрена;
- система контроля за удаленным доступом: используются стандартные механизмы контроля: аутентификация по логину и паролю, фильтрация IP-адресов силами сетевого экрана. Специализированное программное решение такого рода не используется.

3.5. Оператор на основании договора может поручить обработку персональных данных третьему лицу. Существенным условием такого договора является наличие права у данного лица на обработку персональных данных, обязанность соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

4. Сроки обработки и хранения персональных данных

4.1. Обработка персональных данных в Организации прекращается в следующих случаях:

- при выявлении факта неправомерной обработки персональных данных. Срок прекращения обработки - в течение 3 рабочих дней с даты выявления такого факта;
- при достижении целей их обработки (за некоторыми исключениями);
- по истечении срока действия или при отзыве субъектом персональных данных согласия на обработку его персональных данных (за некоторыми исключениями), если в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» их обработка допускается только с согласия;
- при обращении субъекта персональных данных к Организации с требованием о прекращении обработки персональных данных (за исключением случаев, предусмотренных ч. 5.1 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»). Срок прекращения обработки - не более 10 рабочих дней с даты получения требования (с возможностью продления не более чем на 5 рабочих дней, если направлено уведомление о причинах продления).

4.2. Персональные данные хранятся в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Исключение - случаи, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем, по которому) является субъект персональных данных.

4.3. Персональные данные на бумажных носителях хранятся в Организации в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в Российской Федерации (Федеральный закон от 22.10.2004 № 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 № 236)).

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

4.5. Работнику Оператора, имеющему право осуществлять обработку персональных данных, предоставляются уникальный логин и пароль для доступа к соответствующей информационной системе Оператора в установленном порядке. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными регламентами Оператора.

Информация может вноситься как в автоматическом режиме - при уточнении, извлечении, использовании и передаче на машиночитаемом носителе информации, так и в ручном режиме - при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

5. Передача персональных данных

5.1. При передаче персональных данных субъектов Оператор должен соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных Трудовым кодексом Российской Федерации и иными федеральными законами;

- не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами;

- осуществлять передачу персональных данных в пределах Организации в соответствии с настоящим Положением, с которым работник должен быть ознакомлен под подпись;

- разрешать доступ к персональным данным работников только лицам, указанным в разд. 7 Положения, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работников, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции

(для отдельных категорий работников);

- передавать персональные данные работников представителям работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

6. Защита персональных данных

6.1. Оператор до начала обработки персональных данных назначает ответственного за организацию обработки персональных данных (далее - куратор ОПД).

6.2. Обработку персональных данных организует генеральный директор, который является ответственным ОПД и куратором ОПД.

6.3. Служба ОПД находится в непосредственном подчинении куратора ОПД - лица, ответственного за организацию обработки персональных данных в Организации.

6.4. Куратор ОПД:

1) доводит до сведения работников Оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

2) организует обработку персональных данных работниками Оператора;

3) организует прием и обработку обращений и запросов субъектов персональных данных или их представителей.

6.5. Контроль за исполнением работниками Оператора требований законодательства Российской Федерации и положений локальных нормативных актов Оператора при обработке персональных данных возложен на генерального директора.

6.6. В рамках внутреннего контроля генеральный директор:

1) осуществляет внутренний контроль за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) контролирует прием и обработку обращений и запросов субъектов персональных данных или их представителей.

6.7. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах Оператора, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных,

необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Постановлением Правительства РФ от 01.11.2012 № 1119 уровни защищенности персональных данных;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- применение для уничтожения персональных данных, прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации;

- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учет машинных носителей персональных данных;

- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.8. При обработке Организацией персональных данных в информационных системах актуальны угрозы 1 (первого) типа.

6.9. Для обеспечения 1 (первого) уровня защищенности персональных данных при их обработке в информационных системах установлены следующие меры:

6.9.1. В помещениях с размещенной информационной системой доступ ограничен следующим образом: установлены замки, сигнализация и видеокамеры).

6.9.2. Носители персональных данных хранятся следующим образом: в сейфе.

6.9.3. Организация применяет следующие средства защиты персональных данных, прошедшие процедуру оценки соответствия установленным требованиям: антивирусное ПО, СКЗИ, сетевые экраны, шифрование каналов связи.

6.9.4. В электронном журнале безопасности автоматически регистрируются изменения полномочий работника Организации по доступу к персональным данным, содержащимся в информационных системах.

Ответственным за обеспечение безопасности персональных данных в информационных системах, является генеральный директор.

6.5. Контроль за выполнением Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, проводится в следующие сроки: не реже 1 раза в 3 года в следующем порядке: ответственное лицо организует и проводит контроль самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

6.6. В целях защиты персональных данных субъектов при их обработке, осуществляемой без использования средств автоматизации, применяются следующие меры:

6.6.1. Документы, содержащие персональные данные субъектов, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

6.6.2. Помещения, в которых хранятся персональные данные, оборудуются сигнализацией и видеокамерами.

6.7. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов, Организация обязана с момента выявления такого инцидента им, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в порядке, предусмотренном ч. 3.1 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ № «О персональных данных». При направлении уведомления следует руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными Приказом Роскомнадзора от 14.11.2022 № 187.

6.8. Организация обязана в Порядке, утвержденном Приказом ФСБ России от 13.02.2023 № 77, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

7. Порядок уничтожения персональных данных

7.1. При достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей персональные данные уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.

7.2. Незаконно полученные персональные данные или те, которые не являются необходимыми для цели обработки, уничтожаются в течение 7 рабочих дней со дня представления субъектом персональных данных (его представителем) подтверждающих сведений.

7.3. Персональные данные, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления факта неправомерной обработки.

7.4. Персональные данные уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иным соглашением между ним

и Организацией либо если Организация не вправе обрабатывать персональные данные без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

7.5. При достижении максимальных сроков хранения документов, содержащих персональные данные, персональные данные уничтожаются в течение 30 дней.

7.6. Персональные данные уничтожаются (если их сохранение не требуется для целей обработки персональных данных) в течение 30 дней с даты поступления отзыва субъектом персональных данных согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем, по которому) является субъект персональных данных, иное соглашение между ним и Организацией. Кроме того, персональные данные уничтожаются в указанный срок, если Организация не вправе обрабатывать их без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

7.7. Отбор материальных носителей (документы, жесткие диски, флеш-накопители и т.п.) и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению, осуществляет Ответственный ОПД.

7.8. Уничтожение персональных данных осуществляет комиссия, созданная приказом генерального директора Организации.

7.8.1. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

7.8.2. Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

7.8.3. Комиссия подтверждает уничтожение персональных данных согласно Требованиям к подтверждению уничтожения персональных данных, утвержденным Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных - если данные обрабатываются без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных - если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, которые должны содержаться в указанных документах, утверждаются приказом руководителя Организации.

7.8.4. Акты и выгрузки из журнала хранятся в течение 3 лет с момента уничтожения персональных данных.

8. Контроль, ответственность за нарушение или неисполнение Положения

8.1. Контроль за исполнением Положения возложен на генерального директора.

8.2. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами. Кроме того, они привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном законодательством Российской Федерации.

8.3. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к их защите, установленных Федеральным законом от 27.07.2006 № 152-ФЗ № «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

8.4. Руководители структурных подразделений Оператора несут персональную ответственность за исполнение обязанностей их подчиненными.