УТВЕРЖДЕНО
приказом от 21.05.2025 № 8

Положение
о процедурах, направленных на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений

1. Положение о процедурах, направленных на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений (далее – Положение) разработано в Обществе с ограниченной ответственностью «Клиника 32» (далее – Общество, Оператор) во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон).

2. Оператор осуществляет обработку персональных данных, основываясь на следующих принципах обработки:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей; обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается;

- объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой, не допускается;

- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки, а обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных; Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

- хранение персональных данных осуществляется 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.

3. Оператором определены меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом, принятыми в соответствии ним нормативными правовыми актами:

- назначено лицо, ответственное в Обществе за организацию обработки персональных данных;

- Оператором издан документ, определяющий политику в отношении обработки персональных данных, обеспечена возможность доступа к указанному документу с использованием средств информационно-телекоммуникационной сети «Интернет»;

- издан акт по вопросам обработки персональных данных, в котором для каждой цели обработки персональных данных определены категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, а также порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований;

- издан локальный акт, устанавливающий процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

- определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

- применяются организационные и технические меры 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 Правительством Российской Федерации уровни защищенности персональных данных;

- применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;

- произведен учет машинных носителей персональных данных;

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

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

- обеспечены средства для восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установлены правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечены регистрация и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- производится контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных;

- осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных положениям Закона и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике в отношении обработки персональных данных, локальным актам Общества;

- осуществляется оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, соотношение причиненного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом;

- работники Общества, непосредственно осуществляющие обработку персональных данных, ознакомлены 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 актами по вопросам обработки персональных данных.

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

5. К обязанностям Оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных, в частности, относятся следующие:

5.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу уполномоченного органа по защите прав субъектов персональных данных (далее – Роскомнадзор) Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, либо обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) – с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по его поручению, Оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по его поручению. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос Роскомнадзора были направлены Роскомнадзором, также уведомляет указанный орган.

5.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор блокирует персональные данные, относящиеся к этому субъекту персональных данных, либо обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) – 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 либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) – в течение 7 (семи) рабочих дней со дня представления таких сведений и снимает блокировку персональных данных.

5.3. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор с момента выявления такого инцидента Оператором, Роскомнадзором или иным заинтересованным лицом, направляет в Роскомнадзор уведомления о таких фактах: первичное и дополнительное.

5.3.1. Информацию о произошедшем инциденте (первичное уведомление) – в течение 24 (двадцати четырех) часов.

Первичное уведомление должно содержать сведения о:

- о произошедшем инциденте (дату и время выявления инцидента, характеристику (характеристики) персональных данных (содержание базы данных, ставшей доступной неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных (далее – скомпрометированная база данных), количество содержащихся в ней записей. Дополнительно Оператор может представить информацию об актуальности скомпрометированной базы данных, а также о периоде, в течение которого собраны персональные данные);

- о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных (предварительные причины неправомерного распространения персональных данных, повлекшего нарушение прав субъектов персональных данных);

- о предполагаемом вреде, нанесенном правам субъектов персональных данных (результаты предварительной оценки вреда, который может быть нанесен субъектам персональных данных, в связи с неправомерным распространением персональных данных, а также последствия такого вреда, проведенной в соответствии с п. 5 ч. 1 ст. 18.1 Закона);

- о принятых мерах по устранению последствий соответствующего инцидента (перечень принятых Оператором организационных и технических мер по устранению последствий инцидента в соответствии со ст.ст. 18.1, 19 Закона);

- о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором, по вопросам, связанным с выявленным инцидентом;

- данные Оператора, направившего уведомление в соответствии с перечнем, предусмотренным п. 2.2 Порядка и условий 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, утвержденным приказом Роскомнадзора от 14.11.2022 № 187 (далее – Порядок);

- иные сведения и материалы, находящиеся в распоряжении Оператора, в том числе об источнике получения информации об инциденте, а также подтверждающие принятие мер по устранению последствий инцидента (при наличии).

В случае если Оператор на момент направления первичного уведомления располагает сведениями о результатах внутреннего расследования выявленного инцидента, то он вправе указать такие сведения в первичном уведомлении.

5.3.2. Информацию о результатах внутреннего расследования выявленного инцидента (дополнительное уведомление) – в течение 72 (семидесяти двух) часов – о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Дополнительное уведомление должно содержать сведения:

- о результатах внутреннего расследования выявленного инцидента (информация о причинах, повлекших нарушение прав субъектов персональных данных, и вреде, нанесенном правам субъектов персональных данных, о дополнительно принятых мерах по устранению последствий соответствующего инцидента (при наличии), а также о решении Оператора о проведении внутреннего расследования с указанием его реквизитов);

- о лицах, действия которых стали причиной выявленного инцидента (при наличии) (фамилия, имя, отчество (при наличии) должностного лица Оператора с указанием должности (если причиной инцидента стали действия сотрудника Оператора), фамилия, имя, отчество (при наличии) физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной выявленного инцидента, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц и (или) устройств (если причиной инцидента стали действия посторонних лиц) и иные сведения о выявленном инциденте, имеющиеся в распоряжении Оператора).

5.3.3. Первичное и дополнительное уведомления направляются в виде документа на бумажном носителе или в форме электронного документа. Требования к направлению указанных уведомлений установлены в п.п. 6, 7 Порядка.

5.3.4. Оператору с момента поступления в Роскомнадзор по адресу электронной почты, указанному в первичном уведомлении, направляется информационное письмо, содержащее сведения о дате и времени передачи уведомления в информационную систему Роскомнадзора, а также номер и ключ уведомления.

При направлении дополнительного уведомления посредством Портала персональных данных Оператор должен указать номер и ключ первичного уведомления.

5.3.5. В случае направления Оператором неполных или некорректных сведений Роскомнадзор по адресу электронной почты, указанному в первичном уведомлении, не позднее 3 (трех) рабочих дней со дня получения первичного или дополнительного уведомления направляет запрос Оператору о предоставлении недостающих сведений и (или) пояснений относительно некорректности представленных в уведомлении сведений.

Недостающие сведения и (или) пояснения относительно некорректности представленных данных должны быть представлены Оператором в Роскомнадзор в течение 3 (трех) рабочих дней со дня получения запроса от Роскомнадзора одним из способов, предусмотренных пп. 5.3.3. настоящего Положения.

5.3.6. В случае непоступления дополнительного уведомления в адрес Роскомнадзора в течение 72 часов, Оператору направляется требование о необходимости представить сведения о результатах внутреннего расследования выявленного инцидента.

Ответ на указанное требование направляется Оператором Роскомнадзору в течение 1 (одного) рабочего дня со дня получения такого требования одним из способов, предусмотренных пп. 5.3.3. настоящего Положения.

5.3.7. В случае если Роскомнадзором выявлен факт неправомерного распространения скомпрометированной базы данных, содержание которой указывает на ее принадлежность к конкретному оператору, такому оператору направляется требование о необходимости представить уведомление.

Оператор, которому направлено указанное требование, направляет его в Роскомнадзор в сроки, установленные ч. 3.1 ст. 21 Закона.

5.3.8. В случае неподтверждения оператором факта, указанного в пп. 5.3.7 настоящего Положения, указанному оператору при выявлении такого инцидента Роскомнадзором или иным заинтересованным лицом, оператором направляется уведомление, предусмотренное ч. 3.1 ст. 21 Закона.

В таком случае к дополнительному уведомлению Оператором прикладывается акт о проведенном внутреннем расследовании, подтверждающий отсутствие факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, и (или) неустановления принадлежности скомпрометированной базы данных, содержащей персональные данные, соответствующему оператору в деятельности такого оператора.

5.3.9. В случае установления оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайно передачи (предоставления, распространения, доступа) персональных данных, содержащихся в базе данных, характеристики которых полностью соответствуют ранее скомпрометированной базе данных, Оператором направляется уведомление, предусмотренное ч. 3.1 ст. 21 Закона.

В таком случае при направлении уведомления Оператором указывается дата и номер ранее направленного уведомления, содержащего сведения, предусмотренные ч. 3.1 ст. 21 Закона, о ранее скомпрометированной базе данных, содержащей персональные данные.

Генеральный директор _____ / Аветова О.В./