

**ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«АЛЪЯНС КРК»**

(ООО «АЛЪЯНС КРК»)

115409, г. Москва, вн. тер. г. муниципальный округ Москворечье-Сабурово, ш.
Каширское, д. 66, к. 3. тел: 8(495)150-04-26, e-mail: info@alliance-krk.ru, ИНН: 7718312030

УТВЕРЖДЕНО

Генеральный директор
ООО «АЛЪЯНС КРК»

 А.Г. Кузнецов

Редакция 2. Действует с 01 » августа - 2026 г.

**ПОЛИТИКА В ОТНОШЕНИИ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ООО «АЛЪЯНС КРК»**

1. ОБЩИЕ ПОЛОЖЕНИЯ И ОСНОВНЫЕ ПОНЯТИЯ.

1.1. Настоящая Политика общества с ограниченной ответственностью «АЛЪЯНС КРК» в отношении обработки персональных данных (далее - Политика) разработана в исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 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 ООО «АЛЪЯНС КРК» (далее — Оператор, Общество), как с использованием средств автоматизации, так и без использования таких средств.

1.2.1. Общество является медицинской организацией, осуществляющей медицинскую деятельность на основании лицензии по профилям «психиатрия-наркология», «психиатрия», «психотерапия» и иным профилям, предусмотренным лицензией, в условиях стационара, амбулаторно и по месту нахождения пациента.

1.2.2. Сведения о состоянии здоровья пациентов составляют врачебную тайну в значении статьи 13 Федерального закона от 21.11.2011 № 323-ФЗ. Сам факт обращения гражданина за наркологической и психиатрической помощью относится к сведениям, составляющим врачебную тайну. Работники Общества не вправе подтверждать или опровергать факт обращения и нахождения пациента в Обществе любым третьим лицам, кроме случаев, прямо предусмотренных законом или письменным волеизъявлением пациента.

1.2.3. Настоящая Политика является общедоступным документом. Её действующая редакция публикуется на официальных сайтах Общества <https://alliance-krk.ru> и

<https://psy-klinika.ru> и размещается на информационном стенде по месту нахождения Общества.

1.3 Основные понятия, используемые в Политике:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4. Основные права и обязанности Оператора.

1.4.1. Оператор имеет право:

- 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;
- 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;
- 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.

1.4.2. Оператор обязан:

- организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;
- отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;
- 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;
- 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.

1.5. Основные права субъекта персональных данных. Субъект персональных данных имеет право:

- 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;
- 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;
 - выдвигать условие предварительного согласия при обработке персональных данных в целях продвижения на рынке товаров, работ и услуг;
 - обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

2. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

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

2.3. Обработка Оператором персональных данных осуществляется в следующих целях:

- подбор персонала (соискателей) на вакантные должности в Обществе,
- выполнение требований трудового законодательства, ведение кадрового и бухгалтерского учета;
- подготовка, заключение и исполнение гражданско-правовых договоров;
- оказание медицинских услуг, в том числе идентификация пациентов (заказчиков) и их законных представителей, внесение сведений в медицинскую документацию, предоставление сведений страховым компаниям в случае оплаты ими услуг и представление установленной законодательством отчетности;
- оказание медицинской помощи по месту нахождения пациента (вызов врача-нарколога на дом), включая согласование адреса, времени и условий выезда медицинской бригады, а также организацию транспортировки пациента;
- организация записи на приём, в том числе посредством официальных сайтов Общества, телефонной связи и сервисов записи, привлечённых Обществом;
- направление пациентам организационных сообщений, связанных с оказанием медицинских услуг (подтверждение записи, дата и время приёма, напоминание о приёме), посредством телефонной связи, SMS-сообщений и мессенджера, серверы которого расположены на территории Российской Федерации;
- контроль качества обслуживания и обучение персонала посредством записи телефонных разговоров;
- обеспечение безопасности, сохранности имущества и контроль порядка в помещениях Общества посредством видеонаблюдения;
- обработка обращений, заявок, претензий и запросов, поступивших через официальный сайт, по телефону и по электронной почте;

- направление рекламных и информационных сообщений об услугах, акциях и специальных предложениях Общества по сетям электросвязи — при наличии предварительного согласия субъекта персональных данных, оформленного отдельно;

- обеспечение работоспособности и безопасности официальных сайтов Общества; обработка технических данных посетителей; анализ посещаемости сайтов с использованием аналитических файлов cookie при наличии согласия пользователя;

- защита прав и законных интересов Общества, в том числе при взаимодействии с контролирующими и правоохранительными органами и в суде.

- размещение на официальных сайтах Общества сведений о работниках (фамилия, имя, отчество, должность, сведения об образовании, квалификации и стаже, фотография) для информирования пациентов о специалистах — при наличии отдельного согласия на использование изображения и отдельного согласия на обработку персональных данных, разрешённых для распространения.

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

2.5. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

2.7. Случаи, когда для обработки персональных данных не требуется согласие:

- Обработка специальных категорий персональных данных допускается без согласия лица в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну (п.4 ч. 2 ст. 10 Закона № 152-ФЗ).

- Обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

- Обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- Обработка персональных данных необходима для исполнения полномочий и обязанностей, возложенных на Общество законодательством в сфере охраны здоровья граждан, в том числе для ведения медицинской документации и представления отчётности.

Основания, предусмотренные настоящим пунктом, не применяются к обработке персональных данных в целях продвижения услуг Общества. Передача персональных данных третьим лицам осуществляется с согласия субъекта либо без согласия при наличии основания, предусмотренного федеральным законом. Распространение персональных данных осуществляется на основании отдельного согласия, оформленного в соответствии со статьёй 10.1 Федерального закона № 152-ФЗ, если иное прямо не предусмотрено федеральным законом.

3. ПРАВОВОЕ ОСНОВАНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ:

3.1. Правовым основанием для обработки персональных данных в Обществе являются:

- ФЗ «О занятости населения в Российской Федерации» от 12.12.2002 г. №565-ФЗ (ст.52 и ст.53),
- трудовое законодательство Российской Федерации.
- налоговое законодательство Российской Федерации;
- Федеральный закон от 06.12.2011 N 402-ФЗ "О бухгалтерском учете";
- гражданское законодательство Российской Федерации,
- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» и Положение о лицензировании медицинской деятельности;
- Федеральный закон от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе»;
- Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;
- приказ Министерства здравоохранения Российской Федерации от 13.05.2025 № 274н "Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях, оказывающих медицинскую помощь в амбулаторных условиях, и порядков их ведения;
- приказ Министерства здравоохранения Российской Федерации от 03.08.2023 № 408, устанавливающий сроки хранения документов организаций в сфере здравоохранения;
- договоры об оказании платных медицинских услуг, стороной которых является субъект персональных данных;
- Постановление Правительства РФ от 25.03.2015 N 272 "Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)"
- трудовые договоры, локальные акты Общества (в том числе Положение о персональных данных),
- согласие субъекта персональных данных на обработку его персональных данных.

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

4.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разделе 2 настоящей Политики.

4.2. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.3. Общество обрабатывает следующие категории субъектов персональных данных:

4.3.1. Соискатели на вакантные должности.

Категории и перечень обрабатываемых персональных данных:

персональные данные: фамилия, имя, отчество; дата рождения; контактные данные; сведения об образовании, квалификации, опыте и ранее выполняемой работе; иные сведения, включённые соискателем в резюме; фотография — только если соискатель предоставил её добровольно. Фотография соискателя не используется для установления его личности и не обрабатывается как биометрические персональные данные.

4.3.2. Работники, бывшие работники.

Категории и перечень обрабатываемых персональных данных:

фамилия, имя, отчество; год, месяц, дата и место рождения; адрес регистрации и места жительства; семейное положение и состав семьи — в случаях, предусмотренных законом; сведения об образовании и квалификации; доходы; паспортные данные; гражданство; сведения о трудовой деятельности и воинском учёте; СНИЛС; ИНН; данные водительского удостоверения — если управление транспортом входит в трудовую функцию; номер телефона; адрес электронной почты; банковские реквизиты для перечисления выплат; пол; профессия; должность; фотография; сведения о стаже, квалификации и специализации, размещаемые на сайтах Общества при наличии отдельных согласий

специальные категории персональных данных: состояние здоровья необходимое для выполнения трудовой функции,

4.3.3. Члены семьи работников и бывших работников.

Категории и перечень обрабатываемых персональных данных:

непосредственно персональные данные: фамилия, имя, отчество; дата и место рождения, адрес, паспортные данные, контактные данные (номер телефона и эл.почты).

4.3.4. Пациенты Общества;

4.3.5. законные представители пациентов;

4.3.6. лица, направившие заявку или обращение через сайты либо по телефону и не ставшие пациентами;

4.3.7. контрагенты, исполнители и представители контрагентов;

4.3.8. лица, которым пациент разрешил предоставлять сведения, составляющие врачебную тайну.

4.3.9. Работники, пациенты, сопровождающие лица, посетители и иные лица, находящиеся в зонах видеонаблюдения. Обрабатываются изображение, дата, время и место фиксации. Аудиозапись, распознавание лиц и формирование биометрических шаблонов не осуществляются.

4.4. Общество обрабатывает специальные категории персональных данных — сведения о состоянии здоровья пациентов и работников. Сведения о состоянии здоровья пациентов обрабатываются в случаях и на основаниях, предусмотренных статьёй 10 Федерального закона № 152-ФЗ, в том числе без согласия на основании пункта 4 части 2 статьи 10 при одновременном соблюдении установленных им условий, либо на основании письменного согласия, когда оно выступает самостоятельным правовым основанием или прямо требуется законом. Сведения о состоянии здоровья работников

обрабатываются только в объёме, необходимом для определения возможности выполнения трудовой функции и исполнения обязанностей работодателя, предусмотренных законодательством Российской Федерации

4.5. Фотографии и видеозаписи являются персональными данными, если относятся к определённому или определяемому лицу. Они являются биометрическими персональными данными только тогда, когда Оператор использует их для установления личности. Фотографии работников на сайтах и записи обычного видеонаблюдения без распознавания лиц для установления личности не используются и биометрическими персональными данными не являются. Публикация фотографии и иных сведений о работнике на сайте допускается при наличии отдельного согласия на использование изображения в соответствии со статьёй 152.1 Гражданского кодекса Российской Федерации и отдельного согласия на обработку персональных данных, разрешённых субъектом для распространения, в соответствии со статьёй 10.1 Федерального закона № 152-ФЗ. Фотография на пропуске, используемая для установления личности предъявителя, обрабатывается как биометрические персональные данные на основании отдельного письменного согласия работника. Распознавание лиц и формирование биометрических шаблонов Обществом не применяются.

4.6. Обычное видеонаблюдение ведётся в целях обеспечения безопасности, сохранности имущества и контроля порядка на основании пункта 7 части 1 статьи 6 Федерального закона № 152-ФЗ при условии, что права и свободы субъектов не нарушаются. В местах наблюдения размещаются информационные таблички. Камеры не устанавливаются в местах, где лицо вправе рассчитывать на повышенную приватность. Доступ к записям ограничивается; сроки хранения устанавливаются локальным актом с учётом заявленной цели.

5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка персональных данных осуществляется Обществом 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. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.4. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Фонд пенсионного и социального страхования Российской Федерации (Социальный фонд России) и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

5.5. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

5.6. Перечень действий, совершаемых с персональными данными в ООО «АЛЪЯНС КРК»:

- сбор,
- запись,
- систематизация,

- накопление,
- хранение,
- уточнение (обновление, изменение),
- извлечение,
- использование,
- передача (предоставление, доступ), а при наличии отдельного законного основания — распространение. Распространение осуществляется только применительно к данным, целям и ресурсам, указанным в отдельном согласии субъекта либо в федеральном законе
- блокирование,
- удаление,
- уничтожение персональных данных.

5.7. В Обществе применяется смешанный (автоматизированный и неавтоматизированный) способ обработки персональных данных.

5.8. Общество 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:

- 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 Обществе и в структурных подразделениях;
- создает необходимые условия для работы с персональными данными;
- организует учет документов, содержащих персональные данные;
- хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним.

5.9. 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 с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных, в соответствии с ч. 5 ст. 18 Федерального закона "О персональных данных".

5.10. Первичный сбор, запись, систематизация, накопление, хранение, уточнение и извлечение персональных данных граждан Российской Федерации осуществляются с использованием баз данных, находящихся на территории Российской Федерации. Иностранные мессенджеры не используются Обществом для автоматического сбора и передачи сведений о пациентах, сведений о здоровье, содержимого форм и медицинских документов. Сайт может предоставлять пользователю возможность по его выбору перейти во внешний мессенджер. Автоматическая передача за пределы Российской Федерации Widget-ID, UTM-меток и иных персональных данных допускается только после выполнения требований статьи 12 Федерального закона № 152-ФЗ; медицинские сведения через такие интеграции не передаются.

5.11. Запрещается хранить документы с персональными данными и их копии на рабочих местах либо в открытом доступе, а также оставлять шкафы и сейфы открытыми при отсутствии работника в помещении.

5.12. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

5.13. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

5.14. При поручении обработки персональных данных другому лицу договор, оферта или иной документ, на основании которого действует обработчик, должен определять перечень персональных данных, перечень операций, цели обработки, обязанность соблюдать конфиденциальность, требования к защите и локализации данных, обязанность принимать меры, предусмотренные статьями 18.1 и 19 Федерального закона № 152-ФЗ, уведомлять Оператора об инцидентах и предоставлять документы, подтверждающие соблюдение требований. Передача обработчику допускается только в объеме, необходимом для порученной операции.

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

6.1. Подтверждение факта обработки персональных данных Обществом, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Обществом 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.

6.2. 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.

6.3. 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.

6.4. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.5. 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.

6.6. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.7. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Общество 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.

6.8. В случае подтверждения факта неточности персональных данных Общество 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.

6.9. 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.

6.10. 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).

6.11. 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;
- Общество 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 Обществом и субъектом персональных данных.

7. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

7.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

7.2. Обеспечение безопасности при обработке персональных данных Общества, осуществляется в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

7.3. Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.

7.4. Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети интернет, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

7.5. Обеспечение безопасности при обработке персональных данных Общества, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

7.6. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации и технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;

- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

7.7. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы первого типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».

7.8. В соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 уровень защищённости персональных данных — комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определённых угроз безопасности персональных данных при их обработке в информационных системах. При обработке персональных данных в информационных системах устанавливаются четыре уровня защищённости

7.8.1. Перечень информационных систем персональных данных Общества утверждается приказом Общества. Для каждой информационной системы разрабатывается модель угроз безопасности персональных данных и оформляется акт определения уровня защищённости.

7.8.2. Уровень защищённости персональных данных определяется отдельно для каждой информационной системы актом определения уровня защищённости с учётом категорий субъектов и данных, количества субъектов и актуальных типов угроз. Установленный уровень пересматривается при изменении указанных условий.

7.9. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищённости персональных данных, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

8. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ, СВЕДЕНИЯ О ЛИЦАХ, ОТВЕТСТВЕННЫХ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Оператор: общество с ограниченной ответственностью «АЛЪЯНС КРК» (юридический, фактический и почтовый адрес: 115409 г.Москва, внт.тер.г.муниципальный округ Москворечье-Сабурово, Каширское шоссе., д.66 к.3, ИНН: 7718312030, ОГРН: 5147746447382), телефон приемной 8 (800) 707-04-29, адрес эл. почты: info@alliance-krk.ru.

8.2. Ответственные за организацию обработки персональных данных и обеспечение безопасности персональных данных назначаются приказами Общества. Обращения субъектов направляются по адресу Общества или на e-mail: info@alliance-krk.ru.

9. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ОФИЦИАЛЬНОГО САЙТА

9.1. Настоящий раздел применяется к обработке персональных данных пользователей официального сайта Общества <https://alliance-krk.ru>, <https://psy-klinika.ru> (далее — Сайт).

9.2. Персональные данные пользователей Сайта обрабатываются на основании согласия, которое пользователь предоставляет путём самостоятельного проставления отметки в поле «Я даю согласие на обработку персональных данных» перед отправкой формы. Отметка не является предустановленной. Текст согласия доступен по ссылке, размещённой рядом с полем.

9.3. Использование Сайта само по себе не означает согласия пользователя на обработку его персональных данных. Согласие предоставляется отдельным действием пользователя применительно к конкретной форме и конкретным целям.

9.4. Через формы Сайта обрабатываются: имя, указанное пользователем; номер телефона; адрес электронной почты — если предусмотрен конкретной формой; желаемые дата и время приёма; организационный комментарий к записи. При посещении Сайта автоматически обрабатываются IP-адрес, дата и время обращения, адрес запрошенной страницы, источник перехода, сведения о браузере, операционной системе и устройстве, технические ошибки и идентификаторы cookie. После согласия на необязательные технологии могут обрабатываться сведения о просмотрах и действиях на страницах. Содержимое полей форм и переписки не передаётся в системы интернет-аналитики и Yourgood.Widget.

9.5. Формы Сайтов не предназначены для передачи диагноза, симптомов, сведений о лечении и иных сведений о здоровье. Поле организационного комментария должно содержать соответствующее предупреждение. Сведения о здоровье передаются непосредственно медицинскому работнику по установленному Обществом защищённому каналу.

9.6. Файлы cookie используются в следующих целях: технически необходимые — обеспечение работоспособности Сайта, сохранение сессии пользователя, защита от автоматизированных обращений; аналитические — обработка данных о посещении Сайтов, включая cookie-идентификаторы, IP-адрес, сведения о браузере, устройстве,

просмотренных страницах и источнике перехода, для анализа посещаемости и эффективности Сайтов. Аналитические cookie устанавливаются только после отдельного согласия пользователя. Аналитические файлы cookie обрабатываются исключительно при наличии согласия пользователя, выраженного посредством соответствующего элемента интерфейса Сайта.

9.7. Пользователь вправе отказаться от аналитических файлов cookie посредством интерфейса Сайта, а также самостоятельно настроить или отключить приём файлов cookie в браузере. Отказ не влияет на доступность основных функций Сайта.

9.8. На Сайте используется «Яндекс Метрика», счётчик № 36332545, ООО «ЯНДЕКС» (ИНН 7736207543, ОГРН 1027700229193, адрес: 119021, г. Москва, ул. Льва Толстого, д. 16). После согласия обрабатываются IP-адрес, cookie-идентификаторы, сведения о браузере, устройстве, источнике перехода, просмотренных страницах и действиях на них. Функция «Вебвизор» запускается только после согласия; запись содержимого всех полей форм отключается. ООО «ЯНДЕКС» осуществляет обработку в объёме и на условиях, определённых документами сервиса и поручением Оператора.

9.9. SmartCaptcha применяется для защиты форм от автоматизированной отправки в объёме, необходимом для безопасности. Интерактивные «Яндекс Карты» загружаются только после согласия пользователя; до согласия отображается статическая заглушка или текстовый адрес.

9.10. На Сайте используется Yourgood.Widget, предоставляемый российским юридическим лицом ООО «ЙОГУРТ» (ИНН 9731084690, ОГРН 1217700517088, адрес: 121596, г. Москва, ул. Горбунова, д. 2, стр. 3, помещ. 189). После согласия виджет может обрабатывать IP-адрес, cookie-идентификаторы, сведения о браузере, дате и времени посещения, адресах страниц, источнике перехода, UTM-метках, событиях перехода и Widget-ID для отображения каналов связи и учёта переходов. В отношениях по данным посетителей ООО «ЙОГУРТ» привлекается как лицо, осуществляющее обработку по поручению Оператора, в объёме, установленном договором и частью 3 статьи 6 Федерального закона № 152-ФЗ.

9.11. Yourgood.Widget не получает содержимое форм Сайта, телефон, адрес электронной почты, сведения о записи, состоянии здоровья, диагнозе, лечении или медицинскую документацию. Сквозная аналитика с передачей Widget-ID и параметров в CRM либо иностранные мессенджеры отключена, если Оператором не выполнены отдельные законные условия для такой передачи.

9.12. ООО «ЙОГУРТ» является российским лицом, поэтому само подключение виджета не является трансграничной передачей. Переход пользователя в иностранный мессенджер либо автоматическая передача ему Widget-ID, UTM-меток и иных идентификаторов может повлечь трансграничную передачу. Такая функция допускается только после выполнения требований статьи 12 Федерального закона № 152-ФЗ, включая предварительное уведомление Роскомнадзора; сведения о здоровье и иные данные пациентов через такую интеграцию не передаются.

9.13. Сайт может содержать ссылки на сайты третьих лиц. Общество не контролирует обработку персональных данных на таких сайтах; настоящая Политика на них не распространяется.

10. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Персональные данные обрабатываются в течение срока, необходимого для достижения целей обработки, если иной срок не установлен федеральным законом или договором.

10.2. Медицинская документация хранится в сроки, установленные приказом Министерства здравоохранения Российской Федерации от 03.08.2023 № 408. Медицинские карты пациентов психиатрического профиля хранятся 50 лет. Медицинская документация в форме электронных документов хранится 50 лет, если для соответствующего документа не установлен более длительный срок. Срок каждого иного вида документа определяется по соответствующей позиции перечня, утверждённого приказом № 408.

10.3. Соглашения пациентов на обработку персональных данных и информированные добровольные согласия хранятся вместе с медицинской документацией пациента.

10.4. Договоры об оказании платных медицинских услуг, акты и платёжные документы хранятся 5 лет после отчётного года.

10.5. Обращения, заявки и сообщения, поступившие через Сайт и по телефону и не повлёкшие обращения за медицинской помощью, хранятся не более одного года с даты поступления.

10.6. Документы по личному составу, созданные после 1 января 2003 года, хранятся 50 лет. Документы соискателей, не принятых на работу, хранятся 30 дней с даты принятия решения, если от соискателя не получено согласие на более длительное хранение.

10.7. Если Общество осуществляет запись телефонных разговоров, абонент до начала записи уведомляется о записи и её цели. Записи хранятся не более шести месяцев, если конкретная запись не выделена для рассмотрения обращения, претензии или спора.

10.8. Конкретные сроки хранения по видам документов устанавливаются Положением о персональных данных и номенклатурой дел Общества.