

ПИСЬМЕННОЕ СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦИФРОВОЙ СРЕДЕ WRITTEN CONSENT TO THE PROCESSING OF PERSONAL DATA IN THE DIGITAL ENVIRONMENT

Егор Викторович СМОРОДИНОВ

АО «Вкусвилл», Москва, Россия,
evsmorodinov@edu.hse.ru,
ORCID: 0000-0002-6393-4383

Информация об авторе

Е.В. Смородинов — юрист по персональным данным (DPO) АО «Вкусвилл», магистр юриспруденции

Аннотация. Согласие — универсальное основание обработки персональных данных. Его повсеместное использование владельцами интернет-сервисов обусловлено отсутствием формально определенных требований к форме и содержанию. Между тем для обработки отдельных категорий персональных данных необходимо получить согласие в письменной форме, соответствующее определенным законом требованиям. В работе рассматриваются требования российского законодательства к форме и содержанию письменного согласия, а также их влияние на практики владельцев интернет-сервисов в сфере b2c (business to consumer), осуществляющих обработку специальных категорий персональных данных и биометрии, а именно на практики страховых и телемедицинских организаций, владельцев сервисов подбора психологов и сервисов знакомств.

Исследование выявляет основные сложности, связанные с соблюдением требований закона, такие как невозможность изменить перечень лиц, обрабатывающих персональные данные по поручению оператора, без получения нового письменного согласия, сбор излишних персональных данных исключительно для исполнения требований к письменному согласию, затраты на автоматизацию формирования, сбора и учета согласий. Указанные сложности обуславливают отказ владельцев интернет-сервисов в сфере b2c от использования письменных согласий даже в случаях, когда получение письменного согласия необходимо.

- На основе анализа практик владельцев интернет-сервисов предлагаются рекомендации по совершенствованию законодательства, направленные на упрощение требований к письменному согласию.
- Реализация этих рекомендаций позволит операторам снизить административные барьеры и увеличить привлекательность для потребителей сервисов, обрабатывающих специальные категории персональных данных и биометрию.

- **Ключевые слова:** персональные данные, согласие в письменной форме, специальные категории персональных данных, электронная коммерция

- **Для цитирования:** Смородинов Е.В. Письменное согласие на обработку персональных данных в цифровой среде // Труды по интеллектуальной собственности (Works on Intellectual Property). 2025. Т. 54, № 3. С. 22–34; DOI: 10.17323/tis.2025.27960

• Egor V. SMORODINOV

Vkusvill JSC, Moscow, Russia,
evsmorodinov@edu.hse.ru,
• ORCID: 0000-0002-6393-4383

Information about the author

- E.V. Smorodinov — Lawyer for Personal Data (DPO) of Vkusvill JSC, Master of Law

- **Abstract.** Consent is a universal condition for the processing of personal data. Its widespread use by online service providers in Russia is caused by lack of formally defined requirements for its form and content. Meanwhile, in order to process special categories of personal data, it is necessary to obtain written consent in accordance with the requirements defined by Russian legislation. The paper examines the requirements of Russian legislation on the form

and content of written consent, as well as their impact on the practices of b2c online service providers, processing special categories of personal data, including insurance and telemedicine organizations, providers of therapy and dating applications. The study reveals the main difficulties with personal data laws compliance, such as the inability to change the list of processors without obtaining a new written consent, the collection of unnecessary personal data solely for the purpose of fulfilling the requirements for written consent, the costs of automating the creation, collection and accounting of consents. These difficulties cause the b2c online service providers to refuse to use written consents, even in cases where obtaining written consent is necessary. Based on the analysis of the practices of online service providers, recommendations are proposed for simplifying the requirements for written consent. The implementation of these recommendations will allow operators to reduce administrative barriers and increase the attractiveness of services that process sensitive personal data for consumers.

Keywords: personal data, written consent, special categories of personal data, e-commerce

For citation: Smorodinov E.V. Written Consent to the Processing of Personal Data in the Digital Environment // Trudi po Intellectualnoy Sobstvennosti (Works on Intellectual Property). 2025. Vol. 54 (3). P. 22–34; DOI: 10.17323/tis.2025.27960

ВВЕДЕНИЕ

Согласие на обработку персональных данных является единственным универсальным легитимирующим основанием для любого сбора, использования или иных видов обработки персональных данных [1]. По общему правилу согласие может быть получено в любой форме и любым способом. Это позволяет операторам персональных данных использовать согласие субъектов повсеместно, в том числе «для подстраховки», даже в случаях, когда обработка может осуществляться на альтернативном согласии основании. Указанный подход обеспечил широкую распространенность согласий на обработку персональных данных в сфере электронной коммерции.

Тем не менее для обработки, в частности, специальных категорий персональных данных и биометрии оператору недостаточно получить обычное согласие субъекта. Для обработки таких данных требуется согласие, которое соответствует ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон 152-ФЗ) [2]. Хотя соответствующее ч. 4 ст. 9 Закона № 152-ФЗ согласие в литературе называется согласием в письменной форме, оно может быть получено в форме электронного документа. Поэтому операторы, обрабатывающие специальные категории персональных данных и биометрию в рамках интернет-сервисов, также могут использовать согласие в качестве основания для обработки персональных данных, но при условии соблюдения ряда требований. Тем не менее согласие в письменной форме указанными операторами используется крайне редко.

В фокусе статьи — вопрос о том, какое влияние существующее законодательство о персональных данных оказывает на интернет-сервисы, осуществляющие сбор и обработку специальных категорий персональных данных и биометрии. Цель статьи — оценить роль письменного согласия в форме электронного документа как основания для обработки специальных категорий персональных данных в сфере электронной коммерции для поиска путей совершенствования отечественного законодательства о персональных данных.

ПИСЬМЕННОЕ СОГЛАСИЕ КАК ОСНОВАНИЕ, ЛЕГИТИМИРУЮЩЕЕ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Действующие требования к письменному согласию на обработку персональных данных были оформлены в 2011 г. в связи со вступлением в силу Федерального закона от 25.07.2011 № 261-ФЗ и с того момента в ответ на развитие сферы электронной коммерции не изменялись. Данные требования можно разделить на требования к форме и требования к содержанию согласия.

Так, письменное согласие должно быть составлено на бумажном носителе и подписано собственноручно субъектом. Альтернативно, письменное согласие может быть получено в форме электронного документа, подписанного электронной подписью.

Требованием к содержанию письменного согласия является обязательное включение в текст согласия ряда реквизитов, в числе которых:

- фамилия, имя, отчество, адрес и данные документа, удостоверяющего личность субъекта;
- аналогичные данные представителя субъекта, если согласие дает представитель;
- наименование или фамилия, имя и отчество, адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- иные реквизиты, обеспечивающие соответствие согласия требованиям конкретности, информированности, сознательности и однозначности.

Закон дает операторам механизм сбора письменных согласий через интернет путем формирования под каждого пользователя интернет-сервиса отдельного электронного документа с текстом согласия и подписания его электронной подписью. Тем не менее реализация данного механизма на практике приносит ряд издержек и дополнительных рисков, делающих использование письменного согласия как основания обработки персональных данных в b2c-проектах нецелесообразным.

1. Согласие в письменной форме должно формироваться под каждого субъекта персональных данных. Поскольку в ч. 4 ст. 9 Закона 152-ФЗ установлены требования к содержанию согласия, оператору недостаточно получить фамилию, имя и отчество субъекта, его адрес и данные документа, удостоверяющего личность. Эти сведения должны быть включены в текст согласия. Нарушение требований к составу сведений, включаемых в письменное согласие, влечет ответственность по ч. 2 ст. 13.11 Кодекса РФ об административных правонарушениях [3] (размер штрафа за отсутствие одного из обязательных реквизитов согласия тот же, что и за обработку персональных данных в отсутствие согласия).

Отметим сразу два момента. Оператору необходимо понести дополнительные затраты на работников, заполняющих согласия вручную, либо на автоматизацию процесса формирования согласий под каждого субъекта. Также далеко не всегда для предоставления субъекту услуг, предполагающих сбор специальных категорий персональных данных, оператору необходимы адрес регистрации субъекта и его паспортные данные. Включение данных сведений в текст согласия приводит к сбору и обработке излишних персональных данных, что критикуется рядом исследователей [4, 5]. Необходимость сбора дополнительных данных, особенно паспортных данных, помимо прочего снижает конверсию проекта, ограничивает потенциальное количество людей, которые будут готовы воспользоваться услугами проекта [6], а также повышает ущерб, наносимый субъекту в случае утечки, позволяя связать «утекшие» специальные категории персональных данных либо биометрию с конкретным физическим лицом.

2. Оператор обязан вести учет полученных им согласий в письменной форме. В соответствии с ч. 3 ст. 9 Закона 152-ФЗ на оператора возложено бремя доказывания наличия согласия на обработку персональных данных субъекта. Поскольку по общему правилу согласие может быть получено в любой форме и любым способом при условии, что оно соответствует требованиям ч. 1 ст. 9 Закона № 152-ФЗ, операторы свободны в способах доказывания факта получения «обычного» согласия.

Таковыми доказательствами могут выступать, например, лог-файлы, свидетельствующие об активации субъектом чек-бокса согласия на обработку его персональных данных, совершение субъектом действий на сайте, которое невозможно без предоставления владельцу сайта согласия на обработку персональных данных субъекта [1]. Такая свобода в вопросах доказывания позволяет ограничиться простым логированием действий пользователей сайта и не требует от операторов создавать систему учета предоставленных субъектами согласий.

Поскольку к письменному согласию предъявляются требования по содержанию и форме, оператору необходимо доказать не просто факт получения согласия, но факт получения согласия, соответствующего требованиям ч. 4 ст. 9 Закона № 152-ФЗ. Таким образом, оператору, собирающему письменные согласия в форме электронного документа, нужна система учета таких согласий, внедрение которой потребует дополнительных затрат, приведет к созданию дополнительной информационной системы персональных данных, чем увеличит риски утечки персональных данных в организации.

3. Оператор обязан включить в текст согласия в письменной форме реквизиты лиц, осуществляющих обработку персональных данных по поручению, и повторно собирать согласие после изменения перечня обработчиков. Одним из обязательных элементов согласия в письменной форме являются реквизиты лиц, осуществляющих обработку персональных данных по поручению оператора (далее — обработчики). В связи с этим нарушениями являются:

- составление письменного согласия без включения в его текст реквизитов обработчиков либо передача персональных данных для обработки по поручению лицу, чьи реквизиты не указаны в тексте согласия [7–10];
- включение в письменное согласие ссылки на перечень обработчиков, размещенный на сайте оператора [11].

Любое изменение в перечне обработчиков обязывает оператора получать письменное согласие повторно. Иное справедливо для «обычного» согласия. Оператор свободен в определении способов информирования субъекта об обработчиках, в том числе может размещать их перечень на своем сайте, обновлять его без необходимости получать согласие субъекта повторно [11].

Столь ограничивающий операторов подход, применимый к письменному согласию, является значительной проблемой. Необходимо понимать, что ни один современный проект в сфере электронной коммерции не обходится без привлечения обработчиков, таких как хостинг-провайдеры, провайдеры метрических систем и иной аналитики, контекстной рекламы. Функционирование таких проектов не обходится без аутсорсинга даже центральных бизнес-процессов. Так, работа телемедицинских организаций и медицинских страховых организаций невозможна без привлечения медицинских организаций-партнеров, оказывающих очные медицинские услуги.

Существующий подход законодателя и регулятора, требующий от оператора не только указывать в тексте согласия перечень обработчиков, но и заново получать согласие в случае изменения этого перечня, «привязывает» операторов к текущим бизнес-партнерам, препятствует масштабированию проектов путем привлечения новых партнеров-обработчиков, привносит риск невозможности осуществления деятельности проекта на период с момента смены ключевого обработчика (такого, как хостинг-провайдер) до повторного получения от субъектов согласий с измененным перечнем обработчиков.

4. В соответствии с легальным толкованием Закона № 152-ФЗ согласие в письменной форме должно быть подписано усиленной квалифицированной электронной подписью. Из буквального толкования закона следует, что письменное согласие в форме элек-

тронного документа может быть подписано любой электронной подписью, установленной законом. Тем не менее указанная позиция не столь однозначна.

Действующая редакция ч. 4 ст. 9 Закона 152-ФЗ появилась в 2011 г., уже после принятия, но до вступления в силу Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее — ФЗ «Об электронной подписи») [12]. Такая хронология вступления в силу указанных изменений породила неопределенность в части распространения на ч. 4 ст. 9 Закона № 152-ФЗ переходных положений ч. 3 ст. 19 ФЗ «Об электронной подписи»: «В случаях, если федеральными законами, вступившими в силу до 1 июля 2013 г., предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись...»

Из публичных разъяснений Роскомнадзора следует, что указанные переходные положения следует применять и к ч. 4 ст. 9 Закона № 152-ФЗ, в связи с чем согласие должно подписываться усиленной квалифицированной электронной подписью [13]. Отметим, что в более поздних, но частных разъяснениях ведомство скорректировало свою позицию, допустив использование вместо квалифицированной подписи простую электронную [14], однако обозначенная публично позиция скорректирована так и не была.

Позиция о допустимости подписания согласий простой электронной подписью разделяется как территориальными управлениями ведомства, так и судами [15]. Тем не менее единственное легальное толкование закона скорректировано не было, что позволяет говорить о сохранении неопределенности и риске изменения практики регулятора и судов в сторону запрета на подписание письменного согласия простой электронной подписью.

Вывод. Таким образом, письменное согласие не является удобным для операторов легитимирующим основанием для обработки персональных данных при его предоставлении в форме электронного документа.

Важно отметить, что каждый из рассмотренных в разделе нюансов работы с письменными согласиями преодолим. На рынке присутствуют решения как по автоматическому формированию документов, так и по учету согласий на обработку персональных данных. При этом внедрение таких решений не влияет значительно на пользовательский путь субъекта персональных данных, в том числе благодаря использованию простой электронной подписи (представляющей собой зачастую сочетание логина и пароля) для подписания согласий.

Тем не менее значительно затрудняют использование письменного согласия требования по сбору дополнительных персональных данных субъекта и необходимость повторного получения согласия при

изменении перечня обработчиков. Иными словами, использование письменного согласия снижает конверсию проекта, приводит к излишнему накоплению персональных данных, ограничивает возможности масштабирования бизнеса и привносит риск остановки работы проекта при смене ключевых обработчиков.

Из рассмотрения требований к письменному согласию становится очевидно, что только два из всех предусмотренных законодательством РФ требований к письменному согласию способствуют защите прав субъектов, а именно :

- требование указывать информацию о процессе обработки (цель, способы и сроки обработки, перечень обрабатываемых персональных данных, реквизиты обработчиков);
- требование повторно получать согласие при изменении перечня обработчиков.

При этом первое требование к письменному согласию фактически предъявляется и к «обычному» согласию, поскольку отсутствие этих сведений в согласии (если оно составлено отдельным документом) или в политике конфиденциальности (если согласие не составлено отдельным документом, а субъект соглашается на обработку персональных данных на условиях политики) нарушило бы принцип информированности согласия. Второе требование предоставляет субъекту персональных данных минимальный контроль за тем, каким лицам будут раскрыты его персональные данные. Тем не менее на практике отказ субъекта от предоставления согласия на обработку его персональных данных при смене перечня обработчиков будет означать невозможность использования субъектом сервиса оператора, ведь согласие в подавляющем большинстве случаев является условием предоставления субъекту сервисов [16, 17].

Это сводит к минимуму ценность письменного согласия как инструмента защиты прав субъектов персональных данных. Вот почему заслуживают критики позиции тех исследователей, которые заявляют о необходимости распространить обязательное предоставление письменных согласий, например, на случаи обработки персональных данных нейросетями [18], или на всю обработку, осуществляемую на основании согласия [19, 20].

АНАЛИЗ ПРАКТИК ОПЕРАТОРОВ, ОБРАБАТЫВАЮЩИХ СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОКАЗАНИИ УСЛУГ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-СЕРВИСОВ

Чтобы оценить влияние обозначенных особенностей работы с письменными согласиями при их сборе

в форме электронных документов, недостаточно теоретического анализа. Необходимо рассмотреть практики операторов по легитимации обработки персональных данных. Обработка специальных категорий персональных данных может осуществляться рядом интернет-сервисов, например сервисами знакомств, форумами, интернет-сервисами, обрабатывающими сведения о состоянии здоровья (сервисами страховых организаций, телемедицинскими сервисами, сервисами подбора психологов).

В ходе анализа пользовательского пути указанных интернет-сервисов, рассмотрения текста политик обработки персональных данных и согласий, собираемых посредством сервиса, было выделено три основных подхода к легитимации обработки специальных категорий персональных данных:

- получение согласия, не соответствующего требованиям ч. 4 ст. 9 Закона № 152-ФЗ, для обработки специальных категорий персональных данных;
- легитимация обработки персональных данных с использованием альтернативных согласию оснований обработки;
- игнорирование факта сбора специальных категорий персональных данных.

ИНТЕРНЕТ-СЕРВИСЫ СТРАХОВЫХ ОРГАНИЗАЦИЙ

Интернет-сервисы страховых компаний позволяют организовать дистанционное взаимодействие между страховщиком, страхователем, застрахованным лицом и лицом, имеющим право на страховое возмещение. Интернет-сервисы могут использоваться страховщиками для сбора сведений о наступлении страхового случая, для получения страхового возмещения, в том числе для записи в медицинскую организацию при получении медицинской помощи по полису добровольного медицинского страхования (далее также — ДМС).

Для получения этих сведений страховщики используют мобильные приложения и специальные формы сбора сведений на сайтах страховщиков. Так, ООО СК «Сбербанк страхование» (далее — «Сберстрахование») собирает сведения о страховом случае через онлайн-помощника [21]. Аналогичный функционал есть в мобильном приложении СПАО «Ингосстрах» (далее — «Ингосстарх») [22], в мобильном приложении и на сайте АО «АльфаСтрахование» (далее — «АльфаСтрахование») [23]. Для использования всех трех сервисов необходимо предоставить согласие на обработку персональных данных, в том числе сведений о состоянии здоровья. Тем не менее ни одно из собираемых страховщиками согласий не соответствует требованиям, предъявляемым к пись-

менному согласию. Так, согласие, предоставляемое при оформлении полиса ДМС на сайте «СберСтрахования», не формируется под каждого субъекта и не содержит в своем тексте список обработчиков, а только ссылку на него [24]. Согласие, собираемое компанией «АльфаСтрахование» [25] на этапе оформления полиса ДМС, также не формируется под каждого субъекта и только отсылает к перечню обработчиков. Согласие, получаемое «Ингосстрахом», включено в текст договора ДМС, который субъект должен заполнить собственноручно. Соответственно, в тексте согласия присутствуют такие сведения, как фамилия, имя и отчество, паспортные данные субъекта, его адрес. Тем не менее в тексте указанного согласия нет перечня обработчиков и оно не подписывается электронной подписью, поскольку в соответствии с законом договор страхования в форме электронного документа может быть заключен исключительно конклюдентными действиями путем оплаты страхового полиса [26, ст. 6.1].

Таким образом, каждый из рассмотренных страховщиков использует согласие как основание для обработки персональных данных, в том числе персональных данных специальных категорий, являющихся сведениями о состоянии здоровья. Однако собираемые рассмотренными страховщиками согласия не являются письменными согласиями.

Необходимо отметить, что страховщики могут осуществлять обработку специальных категорий персональных данных на основании страхового законодательства [2, п. 8 ч. 2 ст. 10]. В связи с этим согласие не требуется, например, для сбора сведений о страховом случае от страхователя или выгодоприобретателя, поскольку обязанность по предоставлению указанных сведений прямо возложена на этих лиц законом [27, ст. 961].

Тем не менее не любой сбор или обмен персональными данными осуществляется страховщиками на основании предусмотренных законом прав и обязанностей. Так, взаимодействие страховщиков и медицинских организаций в рамках исполнения договоров ДМС построено на обмене реестрами данных, а именно реестрами застрахованных лиц и реестрами данных об услугах, оказанных медицинскими организациями застрахованным лицам. Первые позволяют страховщикам информировать медицинские организации о лицах, имеющих право обратиться за медицинской помощью. На основании вторых определяется вознаграждение медицинской организации по окончании отчетного периода, в котором она оказывала медицинские услуги застрахованным у страховщика лицам.

Реестры данных об услугах могут содержать информацию о дате и времени посещения застрахован-

ным лицом медицинской организации, об оказанных застрахованному услугах, о поставленном диагнозе с кодами международной классификации болезней. Получение от медицинских организаций указанных сведений для целей приемки и оплаты оказанных медицинскими организациями услуг прямо не предусмотрено страховым законодательством, в связи с чем из закона не следует, что обработка персональных данных в указанных целях может осуществляться на альтернативном письменному согласию основании.

Кроме того, страховые организации могут привлекать хостинг-провайдеров для хранения персональных данных застрахованных лиц, в том числе сведений о состоянии их здоровья. Например, рассмотренные выше страховщики, собирающие сведения о состоянии здоровья через свои сайты, прибегают к услугам хостинг-провайдеров. По данным reg.ru, сайт «АльфаСтрахования» размещен на серверах ПАО «МТС» [28], а сайт «СберСтрахования» — на серверах ООО «Облачные технологии» [29].

Таким образом, не все случаи обработки персональных данных о состоянии здоровья в рамках договоров страхования могут полноценно покрываться альтернативным письменному согласию основанием обработки. Тем не менее страховщики не спешат внедрять сбор письменных согласий в пользовательский путь своих мобильных приложений и сайтов, опираясь на обычные согласия для легитимации обработки персональных данных о состоянии здоровья застрахованных лиц.

ИНТЕРНЕТ-СЕРВИСЫ ТЕЛЕМЕДИЦИНСКИХ ОРГАНИЗАЦИЙ

Интернет-сервисы телемедицинских организаций используются для коммуникации между телемедицинской организацией и заказчиком ее услуг. Как и страховые организации, телемедицинские организации осуществляют через интернет-сервисы сбор персональных данных специальных категорий, например, в ходе онлайн-консультаций с врачом, а также обмениваются персональными данными с лечебно-профилактическими учреждениями, чтобы принять оказанные пациенту лечебно-профилактическим учреждением услуги и предоставить пациенту доступ к результатам анализов и иных проведенных очно обследований.

Телемедицинские организации, как и страховые организации, могут использовать альтернативное согласию основание для обработки персональных данных в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг [2, ст. 10, ч. 2,

п. 4]. Тем не менее осуществлять обработку по данному основанию могут только лица, обязанные сохранять врачебную тайну. Такими лицами в соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» являются медицинские организации и медицинские работники. Из содержания закона неясно, могут ли иные сотрудники медицинской организации, не являющиеся медицинскими работниками, обрабатывать сведения о состоянии здоровья без согласия субъекта, ведь для раскрытия таким работникам сведений о состоянии здоровья в рамках режима врачебной тайны согласие на раскрытие врачебной тайны необходимо [30, ст. 13, ч. 3].

Поскольку телемедицинские сервисы предполагают дистанционное взаимодействие пациента и врача, записи онлайн-консультаций, чатов, отчетов врача могут быть доступны техническим специалистам для исправления ошибок в работе сервиса и его улучшения. Кроме того, доступ к персональным данным могут иметь сотрудники отдела контроля качества. Согласие на обработку сведений о состоянии здоровья в указанных целях получают, например, ООО «ДМО» (далее — «Доктис») [31] и ООО «Мобильные Медицинские Технологии» (далее — «Онлайн Доктор») [32].

Кроме того, из закона не следует, может ли телемедицинская организация передавать медицинским организациям-партнерам персональные данные на рассматриваемом альтернативном основании. Как и в случае с работниками медицинской организации, которые не являются врачами, для передачи сведений, составляющих врачебную тайну, другой медицинской организации необходимо получить согласие на раскрытие врачебной тайны от пациента. Однозначно, согласие на обработку сведений о состоянии здоровья необходимо в случае привлечения хостинг-провайдеров для хранения персональных данных пользователей телемедицинского сервиса.

Таким образом, подходящее для телемедицинских организаций альтернативное согласию основание может использоваться в более узком перечне случаев. В отличие от подходящего страховщикам основания, данное основание применимо исключительно при обработке персональных данных врачом и объективно не покрывает все случаи обработки персональных данных телемедицинской организацией и ее партнерами-обработчиками (прежде всего хостинг-провайдерами, такими как ООО «Яндекс» для ООО «Клиника Яндекс.Здоровье» (далее — «Яндекс.Здоровье»)) [33].

Между тем телемедицинские организации не спешат получать от своих пользователей письменные

согласия. Если «Яндекс.Здоровье» прямо в своей политике указывает, что согласие на обработку персональных данных ему не требуется [34], то иные сервисы получают согласие, которое не соответствует требованиям ч. 4 ст. 9 Закона № 152-ФЗ. Так, ООО «ДокДок» (далее — «СберЗдоровье») собирает согласия [35] в момент записи на прием к врачу, однако это согласие не формируется под каждого субъекта, от чего не содержит обязательных для согласия реквизитов. Упомянутые выше «Доктис» и «Онлайн Доктор» собирают согласия в момент регистрации на сервисе. Эти согласия также не формируются под каждого субъекта персональных данных. Интересен подход ООО «Медицинская компания Доктор рядом», разместившего в форме регистрации незаполненное письменное согласие, пригодное для собственноручного подписания на бумаге [36]. Даже если бы эта форма письменного согласия наполнялась персональными данными пользователя по мере его регистрации, сформированное по факту регистрации согласие все равно не соответствовало бы требованиям закона, поскольку на сервисе не предусмотрено подписание документов простой электронной подписью [37].

СЕРВИСЫ ЗНАКОМСТВ И ПОДБОРА ПСИХОЛОГОВ

Сервисы знакомств и подбора психологов могут обрабатывать специальные категории персональных данных для лучшей персонализации, то есть подбора более подходящих пользователю партнеров и психологов. При этом могут собираться сведения о сексуальной ориентации, религиозных, философских и политических убеждениях, о состоянии здоровья, включая психологическое состояние. Хотя психологическое состояние прямо не упоминается в перечне персональных данных специальных категорий или в перечне сведений о состоянии здоровья, приведенном в ст. 22 Федерального закона от 21.11.2011 № 323-ФЗ, относить его к общим персональным данным было бы неверно. В связи с этим ряд исследователей включает психологическое состояние в специальные категории персональных данных [38]. Некоторые сервисы знакомств могут устанавливать личность своих пользователей, используя технологии распознавания лиц [39].

Из этого следует, что функционирование данных сервисов сопряжено с обработкой специальных категорий персональных данных. При этом данные сервисы объединяет то, что российский закон не позволяет им обрабатывать специальные категории персональных данных на альтернативных согласию основаниях.

В связи с этим владельцы данных сервисов обязаны получать письменные согласия своих пользователей для обработки их персональных данных.

Между тем ни один из владельцев рассмотренных ниже сервисов не получает письменных согласий своих пользователей. Вместо этого владельцы сервисов либо указывают на факт обработки специальных категорий персональных данных в своих политиках, игнорируя при этом российское законодательство, либо заявляют об отсутствии на сервисе сбора и обработки таких персональных данных, указывая на это в том числе в тексте политик обработки персональных данных.

К первой категории операторов относятся, например, Tinder LLC, владелец сервиса Tinder, и Online Classifieds AG, владелец сервиса Pure, являющиеся иностранными компаниями. Обе компании создали и опубликовали на своих ресурсах политики обработки сведений о состоянии здоровья [40, 41] во исполнение требований законодательства штатов Вашингтон и Невада, но при этом не внедрили на своих ресурсах механизмы формирования письменных согласий для соблюдения российского законодательства. Ко второй категории относятся сервисы, работающие преимущественно на территории РФ. К ним относятся, например, сервис «VK знакомства», владельцем которого является ООО «В Контакте». Сервис позволяет настроить фильтры выдачи анкет по цели знакомства и полу. В связке указанные настройки выдачи позволяют установить сексуальные предпочтения конкретного пользователя. Несмотря на это, в политике обработки персональных данных проекта факт сбора специальных категорий персональных данных не упоминается [42].

Аналогичную позицию занимают и владельцы российских сервисов подбора психологов, такие как Alter (ООО «Альтер») [43], «Ясно» (ООО «Ясно. лайф») [44], и «Мета» (ООО «Мета») [45]. Для подбора психолога на каждом из сервисов необходимо заполнить входную анкету и сообщить беспокоящие темы, которые хотелось бы обсудить с психологом. Интересна входная анкета сервиса Alter, содержащая такие варианты причин обращения, как: «Большую часть времени я чувствую себя подавленным», «У меня бывают панические атаки» и «У меня суицидальные мысли». Выбор пользователем сервиса варианта из предложенных позволяет оценить его психологическое состояние.

Тем не менее владельцы рассматриваемых сервисов не собирают с пользователей письменных согласий. Такой подход может быть аргументирован тем, что работа психологов не связана с оказанием медицинской помощи, психолог не является специ-

алистом, уполномоченным ставить медицинский диагноз. Поэтому сообщаемые психологу сведения (в том числе собранные посредством входных анкет) не являются анамнезом, а результат консультаций не является результатом оказания медицинской помощи. Однако такой подход не отменяет чувствительности природы собираемых такими сервисами данных и не учитывает, что перечень сведений о состоянии здоровья, закрепленный в законе, является открытым. Соответственно, в конкретном случае к сведениям о состоянии здоровья могут быть отнесены сведения о субъекте, не связанные с оказанием ему медицинских услуг. Иными словами, отказ сервисов подбора психологов от сбора письменных согласий порождает для их владельцев риск привлечения к ответственности за обработку персональных данных специальных категорий без законного основания.

Рассмотрение практик операторов, обрабатывающих специальные категории персональных данных в рамках b2c-сервисов, позволяет прийти к выводу, что такие операторы не легитимируют обработку специальных категорий персональных данных путем получения письменного согласия в форме электронного документа. Вместо получения согласия, соответствующего требованиям ч. 4 ст. 9 Закона № 152-ФЗ, операторы идут на риск привлечения к ответственности за обработку персональных данных без правового основания. Таким образом, предложенный законодателем механизм легитимации обработки, хотя и реализуем теоретически, на практике операторами не применяется.

ЗАКЛЮЧЕНИЕ

Действующее законодательство существенно ограничивает возможность операторов, владеющих интернет-сервисами в сфере b2c, осуществлять обработку персональных данных специальных категорий и биометрии на основании письменного согласия субъектов в форме электронного документа. Существующие ограничения в целом преодолимы, тем не менее их достаточно, чтобы рассмотренные в работе операторы отказывались применять письменное согласие.

Между тем действующие нормы подталкивают операторов использовать согласия для легитимации обработки специальных категорий персональных данных и биометрии. Так, альтернативные согласия основания обработки специальных категорий персональных данных и биометрии не покрывают всех достаточно распространенных в сфере электронной коммерции случаев обработки. Альтернативных согласия оснований не предусмотрено для сервисов подбора психологов, дейтинговых приложений. Кро-

ме того, альтернативные согласию основания обработки персональных данных могут не покрывать всех существенных для оператора, владеющего интернет-сервисом, случаев обработки персональных данных. Так, ими не покрывается передача специальных категорий персональных данных и биометрии хостинг-провайдером, обеспечивающим работу интернет-сервисов и хранящим эти персональные данные по поручению оператора. Наконец, закон создает для операторов состояние неопределенности, поскольку не указывает прямо на возможность отказаться от согласий в пользу альтернативных оснований. В частности, из закона прямо не следует, что обработка персональных данных по поручению может осуществляться на альтернативных согласию основаниях. Также из закона неясно, требуется ли согласие для обмена между медицинскими организациями, между медицинскими организациями и страховщиками сведениями о состоянии здоровья пациента в целях оказания ему медицинских услуг. Операторы при этом далеко не всегда могут опираться на позиции регулятора и судебную практику из-за рисков изменения существующих подходов.

В результате складывается парадоксальная ситуация: операторы собирают с субъектов согласия, но без учета требований к письменному согласию. Из-за недостатков российского законодательства согласие сохраняет для операторов роль основного легитимизирующего основания. При этом операторы не готовы нести издержки по приведению согласий, собираемых через интернет, в соответствие с законными требованиями. Этому способствует пассивность регулятора, снижающая риски привлечения операторов к ответственности и позволяющая откладывать compliance до момента получения требований регулятора об устранении нарушений законодательства, тем самым экономя на нем.

Важно понимать, что сами по себе требования к письменному согласию не способствуют защите интересов субъектов. На это указывает, например, отсутствие аналогичных требований в других правовых порядках, прежде всего в законодательстве Европейского Союза [46]. Как было показано выше, соблюдение требований к письменному согласию в форме электронного документа является прежде всего технической задачей, влияющей на пользовательский путь лишь в части предоставления субъектом дополнительных и зачастую излишних сведений о себе. Кроме того, текущая роль согласия как обязательного условия для получения услуг противоречит сути согласия как свободного волеизъявления субъекта и активно критикуется в литературе [16, 17]. В этом контексте отказ от письменного согласия как неэффективного инструмента защиты интересов субъек-

тов в пользу доработанных и расширенных оснований обработки персональных данных специальных категорий (в первую очередь) и биометрии воспринимается положительно, может способствовать развитию ряда отраслей электронной коммерции.

Тем не менее инициатива полной отмены требований к письменному согласию может критиковаться, поскольку потребует значительной реформы законодательства о персональных данных, внедрения реально работающих механизмов защиты прав субъектов. В связи с этим на текущем этапе возможна отмена наиболее обременительных для операторов положений, а именно требований к содержанию согласия. Из текста согласий относительно безболезненно могут быть исключены:

- реквизиты документа, удостоверяющего личность, как излишне собираемые персональные данные;
- перечень обработчиков персональных данных.

Требование о включении перечня обработчиков в текст согласия должно быть в таком случае заменено требованием об информировании субъекта об изменении перечня обработчиков. Вместе с тем субъекту может быть предоставлено право:

- запретить оператору передавать персональные данные новым обработчикам;
- в упрощенном порядке (через интерфейс сайта/приложения оператора) отозвать согласие при несогласии с изменениями в перечне обработчиков.

СПИСОК ИСТОЧНИКОВ

1. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» // СПС «КонсультантПлюс».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс»;
3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СПС «КонсультантПлюс».
4. Журавлев М.С. Защита персональных данных в телемедицине // Право. Журнал высшей школы экономики. 2016. № 3. С. 72–84.
5. Калачев О.В., Сушильников И.С. Международный опыт использования персональных данных пациентов при телемедицинских консультациях // Военно-медицинский журнал. 2020. Т. 341. № 7. С. 54–56.
6. Malheiros M., Preibusch S. Sign-up or give-up: Exploring user drop-out in web service registration // Symposium on Usable Privacy and Security (SOUPS). 2013.
7. Постановление Девятого арбитражного апелляционного суда от 09.12.2020 по делу № А40-48952/2020.

8. Постановлением Девятого арбитражного апелляционного суда от 30.03.2021 № 09АП-9100/2021.
9. Постановление Девятого арбитражного апелляционного суда от 28.03.2022 № 09АП-85268/2021 по делу № А40-205463/2021.
10. Постановление Арбитражного суда Московского округа от 15.01.2018 по делу № А40-81171/17-149-793.
11. Вебинар Роскомнадзора от 27 июля 2023 г. // [Электронный ресурс]. — URL: https://vk.com/video-76229642_456239470 (дата обращения: 06.10.2024).
12. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ // СПС «Консультант Плюс».
13. Вебинар Роскомнадзора от 26 ноября 2020 г. // [Электронный ресурс]. — URL: https://vk.com/video-76229642_456239243 (дата обращения: 06.10.2024).
14. GDPR&152ФЗ | Коллеги, добрый день // [Электронный ресурс]. — URL: <https://www.facebook.com/groups/gdpr152/permalink/1128821184302321> (дата обращения: 06.10.2024).
15. Решение Арбитражного суда города Санкт-Петербурга и Ленинградской области от 03.06.2024 по делу № А56-26456/2024.
16. Bergemann B. The consent paradox: Accounting for the prominent role of consent in data protection // Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2. 2nd International Summer School, Ispra, Italy, September 4–8, 2017 // Revised Selected Papers 12. 2018. С. 111–131.
17. Zuiderveen Borgesius F.J., Kruikemeier Sanne, Boerman Sophie, Helberger Natali. Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation // Eur. Data Prot. L. Rev. 2017. Т. 3. Р. 353.
18. Минбалева А.В., Сторожакова Е.Э. Проблемы правовой охраны персональных данных в процессе использования нейронных сетей // Вестник Университета имени О.Е. Кутафина. 2023. № 2 (102). — URL: <https://cyberleninka.ru/article/n/problemy-pravovoy-ohrany-personalnyh-dannyh-v-protseesse-ispolzovaniya-neyronnyh-setey> (дата обращения: 08.03.2025).
19. Тарасова Ю.И., Плугарь Д.М. Некоторые проблемы законодательного регулирования защиты персональных данных // Криминалистика. 2023. № 3(44). С. 126–132.
20. Мазина Н.Е., Лазарева А.А. Правовое регулирование процедуры получения согласия на обработку персональных данных // Донецкие чтения 2024: образование, наука, инновации, культура и вызовы современности: материалы IX Международной научной конференции, Донецк, 15–17 октября 2024 г. Донецк: Донецкий государственный университет, 2024. С. 208–210.
21. Сберстрахование. Онлайн-помощник // [Электронный ресурс]. — URL: <https://sberbank-insurance.ru/online-helper/insurance-case> (дата обращения: 06.10.2024).
22. Ингосстрах. Страховой случай ДМС // [Электронный ресурс]. — URL: <https://www.ingos.ru/incident/dms> (дата обращения: 06.10.2024).
23. АльфаСтрахование. Как получить медицинскую помощь при наступлении страхового случая // [Электронный ресурс]. — URL: https://www.alfastrah.ru/accident/need_medical_help/ (дата обращения: 06.10.2024).
24. Согласие на обработку персональных данных для посетителей сайта // [Электронный ресурс]. — URL: https://sberbank-insurance.ru/i/docs/political-personal-data_2.pdf (дата обращения: 06.10.2024).
25. Согласие на обработку персональных данных // [Электронный ресурс]. — URL: https://www.alfastrah.ru/docs/soglasie_pd.pdf (дата обращения: 06.10.2024).
26. Закон РФ от 27.11.1992 № 4015–1 «Об организации страхового дела в Российской Федерации» // СПС «Консультант Плюс».
27. Гражданский кодекс Российской Федерации. Часть 2 от 26 января 1996 г. № 14-ФЗ // СПС «Консультант Плюс».
28. Reg.ru. Whois-сервис // [Электронный ресурс]. — URL: <https://www.reg.ru/whois/?dname=www.alfastrah.ru&csrf=58eaf877b61e3a77b08f2c58da5af7c7> (дата обращения: 06.10.2024).
29. Reg.ru. Whois-сервис // [Электронный ресурс]. — URL: <https://www.reg.ru/whois/sberbankins.ru> (дата обращения: 06.10.2024).
30. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // СПС «Консультант Плюс».
31. Согласие на обработку персональных данных и сведений, отнесенных к врачебной тайне // [Электронный ресурс]. — URL: <https://files.server.doctis.ru/content/personal-data-consent.pdf> (дата обращения: 06.10.2024).
32. Согласие на обработку персональных данных и передачу информации, составляющей врачебную тайну // [Электронный ресурс]. — URL: <https://onlinedoctor.ru/privacy/contract2/> (дата обращения: 06.10.2024).
33. Reg.ru. Whois-сервис // [Электронный ресурс]. — URL: <https://www.reg.ru/whois/?dname=health.yandex.ru> (дата обращения: 06.10.2024).
34. Политика ООО «Клиника Яндекс.Здоровье» в отношении обработки персональных данных и сведения

о реализуемых требованиях к защите персональных данных // [Электронный ресурс]. — URL: https://yandex.ru/legal/kyz_privacy/ (дата обращения: 06.10.2024).

35. Согласие на обработку персональных данных при использовании сервиса записи «СберЗдоровье» // «ДокДок» // [Электронный ресурс]. — URL: <https://docdoc.ru/agreement> (дата обращения: 06.10.2024).
36. Согласие на обработку персональных данных // [Электронный ресурс]. — URL: <https://telemed-dr.ru/api/v1/document-agreements/4a9d7aa5-6645-4be6-a264-e5b65473fff2/attached-file> (дата обращения: 06.10.2024).
37. Пользовательское соглашение ООО «МК Доктор рядом» // [Электронный ресурс]. — URL: <https://telemed-dr.ru/api/v1/document-agreements/95b3cfe2-d769-4d19-8937-0f39e52f9d44/attached-file> (дата обращения: 06.10.2024).
38. Гафурова А.Х., Доротенко Е.В., Контемиров Ю.Е. Федеральный закон «О персональных данных»: научно-практический комментарий (постатейный). М.: Ред-я «Российской газеты», 2015. 175 с.
39. Как работает проверка фото? // [Электронный ресурс]. — URL: <https://www.help.tinder.com/hc/ru/articles/4422771431309-Как-работает-проверка-фото> (дата обращения: 06.10.2024).
40. Политика конфиденциальности данных о здоровье потребителей // [Электронный ресурс]. — URL: <https://policies.tinder.com/consumer-health-data-privacy-policy/intl/ru/?lang=ru> (дата обращения: 06.10.2024).
41. Pure's Consumer Health Data Privacy Policy // [Электронный ресурс]. — URL: <https://pure.app/content/en/legal/consumer-health-data-privacy-policy> (дата обращения: 06.10.2024).
42. Политика конфиденциальности VK Знакомства // [Электронный ресурс]. — URL: <https://dating.vk.com/legal/ru/privacy.html> (дата обращения: 06.10.2024).
43. Политика конфиденциальности ООО «Альтер» // [Электронный ресурс]. — URL: https://alter.ru/privacypolicy?alter_campaign=footer (дата обращения: 06.10.2024).
44. Политика в отношении обработки и защиты персональных данных на сервисе «Ясно» // [Электронный ресурс]. — URL: <https://yasno.live/personaldata> (дата обращения: 06.10.2024).
45. Политика конфиденциальности ООО «Мета» // [Электронный ресурс]. — URL: <https://bemeta.co/legal/politics> (дата обращения: 06.10.2024).
46. Регламент Европейского парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональ-

ных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС // СПС «Консультант Плюс».

REFERENCES

1. Savel'ev A.I. Nauchno-prakticheskij postatejnyj kommentarij k Federal'nomu zakonu "O personal'nyh dannyh" // SPS "Konsul'tantPlyus".
2. Federal'nyj zakon ot 27.07.2006 No. 152-FZ "O personal'nyh dannyh" // SPS "Konsul'tant Plyus".
3. Kodeks Rossijskoj Federacii ob administrativnyh pravonarusheniyah ot 30.12.2001 No. 195-FZ // SPS "Konsul'tant Plyus".
4. Zhuravlev M.S. Zashchita personal'nyh dannyh v telemedicine // Pravo. Zhurnal vysshej shkoly ekonomiki. 2016. No. 3. S. 72–84.
5. Kalachev O.V., Sushil'nikov I.S. Mezhdunarodnyj opyt ispol'zovaniya personal'nyh dannyh pacientov pri telemedicinskih konsul'tacijah // Voenno-medicinskij zhurnal. 2020. T. 341, No. 7. P. 54–56.
6. Malheiros M., Preibusch S. Sign-up or give-up: Exploring user drop-out in web service registration // Symposium on Usable Privacy and Security (SOUPS). 2013.
7. Postanovlenie Devyatogo arbitrazhnogo apellyacionnogo suda ot 09.12.2020 po delu No. A40-48952/2020.
8. Postanovleniem Devyatogo arbitrazhnogo apellyacionnogo suda ot 30.03.2021 No. 09AP-9100/2021.
9. Postanovlenie Devyatogo arbitrazhnogo apellyacionnogo suda ot 28.03.2022 No. 09AP-85268/2021 po delu No. A40-205463/2021.
10. Postanovlenie Arbitrazhnogo suda Moskovskogo okruga ot 15.01.2018 po delu No. A40-81171/17-149-793.
11. Vebinar Roskomnadzora ot 27 iyulya 2023 g. // [Elektronnyj resurs]. — URL: https://vk.com/video-76229642_456239470 (data obrashcheniya: 06.10.2024).
12. Federal'nyj zakon "Ob elektronnoj podpisi" ot 06.04.2011 No. 63-FZ // SPS "Konsul'tant Plyus".
13. Vebinar Roskomnadzora ot 26 noyabrya 2020 g. // [Elektronnyj resurs]. — URL: https://vk.com/video-76229642_456239243 (data obrashcheniya: 06.10.2024).
14. GDPR&152FZ | Kollegi, dobryj den' // [Elektronnyj resurs] <https://www.facebook.com/groups/gdpr152/permalink/1128821184302321> (data obrashcheniya: 06.10.2024).
15. Reshenie Arbitrazhnogo suda goroda Sankt-Peterburga i Leningradskoj oblasti ot 03.06.2024 po delu No. A56-26456/2024.

16. Bergemann B. The consent paradox: Accounting for the prominent role of consent in data protection // *Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2. 2nd International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers 12*. 2018. S. 111–131.
17. Zuiderveen *Borgesius F.J., Kruike-meier Sanne, Boerman Sophie, Helberger Natali*. Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation // *Eur. Data Prot. L. Rev.* 2017. T. 3. P. 353.
18. Minbaleev A.V., Storozhakova E.E. Problemy pravovoj ohrany personal'nyh dannyh v processe ispol'zovaniya nejronnyh setej // *Vestnik Universiteta imeni O.E. Kutafina*. 2023. No. 2 (102). — URL: <https://cyberleninka.ru/article/n/problemy-pravovoy-ohrany-personalnyh-dannyh-v-protse-ispolzovaniya-nejronnyh-setej> (data obrashcheniya: 08.03.2025).
19. Tarasova Yu.I., Plugar' D.M. Nekotorye problemy zakonodatel'nogo regulirovaniya zashchity personal'nyh dannyh // *"Kriminalist"*. 2023. No 3(44). S. 126–132.
20. Mazina N.E., Lazareva A.A. Pravovoe regulirovanie procedury polucheniya soglasiya na obrabotku personal'nyh dannyh // *Doneckie chteniya 2024: obrazovanie, nauka, innovacii, kul'tura i vyzovy sovremennosti: materialy IX Mezhdunarodnoj nauchnoj konferencii, Doneck, 15–17 oktyabrya 2024 g.* Doneck: Doneckij gosudarstvennyj universitet, 2024. S. 208–210.
21. Sberstrahovanie. Onlajn-pomoshchnik // [Elektronnyj resurs]. — URL: <https://sberbank-insurance.ru/online-helper/insurance-case> (data obrashcheniya: 06.10.2024).
22. Ingrosstrah. Strahovoj sluchaj DMS // [Elektronnyj resurs]. — URL: <https://www.ingos.ru/incident/dms> (data obrashcheniya: 06.10.2024).
23. Al'faStrahovanie. Kak poluchit' medicinskuyu pomoshch' pri nastuplenii strahovogo sluchaya // [Elektronnyj resurs]. — URL: https://www.alfastrah.ru/accident/need_medical_help/ (data obrashcheniya: 06.10.2024).
24. Soglasie na obrabotku personal'nyh dannyh dlya posetitelej sajta // [Elektronnyj resurs]. — URL: https://sberbank-insurance.ru/i/docs/political-personal-data_2.pdf (data obrashcheniya: 06.10.2024).
25. Soglasie na obrabotku personal'nyh dannyh // [Elektronnyj resurs]. — URL: https://www.alfastrah.ru/docs/soglasie_pd.pdf (data obrashcheniya: 06.10.2024).
26. Zakon RF ot 27.11.1992 № 4015–1 "Ob organizacii strahovogo dela v Rossijskoj Federacii" // SPS "Konsul'tant Plyus".
27. Grazhdanskij kodeks Rossijskoj Federacii, chast' 2 (GK RF ch.2) ot 26 yanvarya 1996 g. No. 14-FZ // SPS "Konsul'tant Plyus".
28. Reg.ru. Whois-servis // [Elektronnyj resurs]. — URL: https://www.reg.ru/whois/?dname=www.alfastrah.ru&_csrf=58eaf877b61e3a77b08f2c58da5af7c7 (data obrashcheniya: 06.10.2024).
29. Reg.ru. Whois-servis // [Elektronnyj resurs]. — URL: <https://www.reg.ru/whois/sberbankins.ru> (data obrashcheniya: 06.10.2024).
30. Federal'nyj zakon ot 21.11.2011 No. 323-FZ "Ob osnovah ohrany zdorov'ya grazhdan v Rossijskoj Federacii" // SPS "Konsul'tant Plyus".
31. Soglasie na obrabotku personal'nyh dannyh i svedenij, otnesennyh k vrachebnoj tajne // [Elektronnyj resurs]. — URL: <https://fileserver.docis.ru/content/personal-data-consent.pdf> (data obrashcheniya: 06.10.2024).
32. Soglasie na obrabotku personal'nyh dannyh I peredachu informacii, sostavlyayushchej vrachebnuyu tajnu // [Elektronnyj resurs]. — URL: <https://onlinedoctor.ru/privacy/contract2/> (data obrashcheniya: 06.10.2024).
33. Reg.ru. Whois-servis // [Elektronnyj resurs]. — URL: <https://www.reg.ru/whois/?dname=health.yandex.ru> (data obrashcheniya: 06.10.2024).
34. Politika OOO "Klinika YAndeks.Zdorov'e" v otnoshenii obrabotki personal'nyh dannyh i svedeniy o realizuemyh trebovaniyah k zashchite personal'nyh dannyh // [Elektronnyj resurs]. — URL: https://yandex.ru/legal/kyz_privacy/ (data obrashcheniya: 06.10.2024).
35. Soglasie na obrabotku personal'nyh dannyh pri ispol'zovanii servisa zapisi "SberZdorov'e" / "DokDok" // [Elektronnyj resurs]. — URL: <https://docdoc.ru/agreement> (data obrashcheniya: 06.10.2024).
36. Soglasie na obrabotku personal'nyh dannyh // [Elektronnyj resurs]. — URL: <https://telemed-dr.ru/api/v1/document-agreements/4a9d7aa5-6645-4be6-a264-e5b65473fff2/attached-file> (data obrashcheniya: 06.10.2024).
37. Pol'zovatel'skoe soglasenie OOO "MK Doktor ryadom" // [Elektronnyj resurs]. — URL: <https://telemed-dr.ru/api/v1/document-agreements/95b3cfe2-d769-4d19-8937-0f39e52f9d44/attached-file> (data obrashcheniya: 06.10.2024).
38. Gafurova A.H., Dorotenko E.V., Kontemirov Yu.E. Federal'nyj zakon "O personal'nyh dannyh": nauchno-prakticheskij kommentarij (postatejnyj). M.: Red. "Ros. Gazety", 2015. 175 s.
39. Kak rabotaet proverka foto? // [Elektronnyj resurs]. — URL: <https://www.help.tinder.com/hc/ru/articles/4422771431309-Kak-rabotaet-proverka-foto> (data obrashcheniya: 06.10.2024).
40. Politika konfidencial'nosti dannyh o zdorov'e potrebitelej // [Elektronnyj resurs]. — URL: <https://>

policies.tinder.com/consumer-health-data-privacy-policy/intl/ru/?lang=ru (data obrashcheniya: 06.10.2024).

41. Pure's Consumer Health Data Privacy Policy // [Elektronnyj resurs]. — URL: <https://pure.app/content/en/legal/consumer-health-data-privacy-policy> (data obrashcheniya: 06.10.2024).
42. Politika konfidencial'nosti VK Znakomstva // [Elektronnyj resurs]. — URL: <https://dating.vk.com/legal/ru/privacy.html> (data obrashcheniya: 06.10.2024).
43. Politika konfidencial'nosti ООО "Al'ter" // [Elektronnyj resurs]. — URL: https://alter.ru/privacypolicy?alter_campaign=footer (data obrashcheniya: 06.10.2024).
44. Politika v otnoshenii obrabotki i zashchity personal'nyh dannyh na servise "Yasno" // [Elektronnyj resurs]. — URL: <https://yasno.live/personaldata> (data obrashcheniya: 06.10.2024).
45. Politika konfidencial'nosti ООО "Meta" // [Elektronnyj resurs]. — URL: <https://bemeta.co/legal/politics> (data obrashcheniya: 06.10.2024).
46. Reglament Evropejskogo parlamenta i Soveta Evropejskogo Soyuza 2016/679 ot 27 aprelya 2016 g. o zashchite fizicheskikh lic pri obrabotke personal'nyh dannyh i o svobodnom obrashchenii takih dannyh, a takzhe ob otmene Direktivy 95/46/ES // SPS "Konsul'tant Plyus".