Утверждено приказом генерального директора
ООО “Сейлбот”
№ 02/11/26-п от 02 ноября 2026 года
в соответствии с ФЗ № 152-фз от 27 июля 2006 года
и другими НПА Российской Федерации

Генеральный директор
_____Гармаш К.Е.

ПОЛИТИКА
ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОДЕРЖАНИЕ

1.(1). ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 3
2. ЦЕЛИ И ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 6
3. СБОР ПЕРСОНАЛЬНЫХ ДАННЫХ И СОГЛАСИЕ НА ИХ ОБРАБОТКУ 7
4. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ 7
5. РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ 9
6. ОБЪЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И УСЛОВИЯ ОБРАБОТКИ 10
7. ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ 13
8. ОТВЕТСТВЕННОСТЬ 15

1.(1). ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.(1).1. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.(1).2. **Оператор персональных данных (оператор)** – 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.

1.(1).3. **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.

1.(1).4. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

1.(1).5. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.(1).6. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.(1).7. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.(1).8. **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.(1).9. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.(1).10. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.(1).11. **Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.(1).12. **Уполномоченный орган** – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по

организации деятельности радиочастотной службы. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных.

1.(1).13. **Персональные данные, разрешенные субъектом персональных данных для распространения,** – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном законодательством Российской Федерации.

1.(1).14. **Согласие на обработку персональных данных** – явно выраженное разрешение субъекта персональных данных на обработку его персональных данных Оператору обработки персональных данных. Согласие может быть выражено как в письменной форме, так и в электронной форме путем осуществления определенных действий на сайте Оператора при регистрации или при участии в партнерской программе путем постановки галочки в чекбоксе рядом с графой “Я согласен на обработку моих персональных данных” с сохранением в log-файлах даты и времени постановки галочки.

1.(1).15. **Клиенты (контрагенты) пользователя (поручителя)** – это лица, персональные данных которых обрабатываются Пользователем с помощью программы для ЭВМ “Сейлбот”. В таком случае пользователь программы для ЭВМ “Сейлбот”, осуществляя услуги через программу для ЭВМ “Сейлбот”, правообладателем которой является ООО “Сейлбот”, фактически является Поручителем для обработки персональных данных, тогда как ООО “Сейлбот” является Поверенным для обработки персональных данных.

1.(1).15.1. Права и обязанности Поручителя и Поверенного, а также иные положения в части, касающейся осуществления обработки персональных данных, сбора согласий на обработку персональных данных клиентов Поручителя, регламентированы в пп. 4.3.1 – 4.3.6 п. 4.3. Настоящей Политики.

1.(1).16. **Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

1.(1).17. **Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

1.(1).18. **Оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

1.(1).19. **Сайт в сети "Интернет"** – совокупность программ для ЭВМ и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет" (далее – Сайт Оператора).

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика обработки и защиты персональных данных определяет порядок обработки и защиты информации о физических лицах - субъектах персональных данных, которые планируют заключить и (или) заключают договоры публичной оферты на оказание услуг и публичной оферты на участие в партнерской программе на сайте Оператора SaleBot.pro (далее – Пользователи) с ОБЩЕСТВОМ С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "СЕЙЛБОТ" (ОГРН 1225800000997, ИНН 5834128222), находящемуся по адресу: Российская Федерация, Пензенская область, г. Пенза, проспект Строителей, д. 39В, помещение № 251 (далее —Оператор).

1.1.2. Общество с ограниченной ответственностью "СЕЙЛБОТ" **включено в реестр операторов обработки персональных** на основании Приказа Уполномоченного органа № 119 от 18.10.2024 г. (регистрационный номер 58-24-007538).

1.2. Целями Политики обработки и защиты персональных данных (далее – Политика) является:

• обеспечение 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, от несанкционированного доступа и разглашения;

• исполнение договоров, заключаемых Оператором с Пользователями;

• предоставление информации об оказываемых Оператором услугах, разработке новых продуктов и услуг;

• исключение несанкционированных действий сотрудников Оператора и любых третьих лиц по сбору, систематизации, накоплению, хранению, уточнению (обновлению, изменению) персональных данных, иных форм незаконного вмешательства в информационные ресурсы и локальную вычислительную сеть Оператора, обеспечение правового и нормативного режима конфиденциальности информации Пользователей.

1.3. Политика описывает каким образом осуществляется обработка персональных данных у Оператора.

1.4. Под обработкой персональных данных подразумеваются любые действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.5. Под персональными данными подразумевается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу – субъекту персональных данных.

1.6. Настоящая Политика разработана в соответствии с действующим законодательством Российской Федерации и Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ. Обработка персональных данных осуществляется с соблюдением принципов и условий, предусмотренных настоящей Политикой и законодательством Российской Федерации в области персональных данных.

1.7. Правовой основой регулирования правоотношений в области обработки и защиты персональных данных, а также в области установления требований по защите и обработке персональных данных выступает Федеральный закон “О персональных данных” от 27.07.2006 № 152-ФЗ.

1.8. Правовым основанием обработки персональных данных в Обществе являются:

1) Совокупность нормативно-правовых актов Российской Федерации, а также иных правовых документов Общества, в соответствии с которыми Общество, выступая в качестве Оператора, осуществляет обработку персональных данных;

2) Публичная оферта Общества;

3) Пользовательское соглашение;

4) Устав оператора;

5) Согласие, явно выраженное субъектом обработки персональных данных;

6) Договоры с контрагентами.

1.7.(3). Оператор обрабатывает персональные в порядке, установленном:

1) Трудовым кодексом Российской Федерации;

2) Федеральным законом от 27.07.2006 № 149-ФЗ “Об информации, информационных технологиях и защите информации”;

3) Федеральным законом от 27.07.2006 № 152-ФЗ “О персональных данных”;

4) Постановлением правительства РФ от 01.11.2012 № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах”;

5) Постановлением правительства РФ от 16.03.2009 № 228 “О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций”;

6) Постановлением Правительства РФ от 15.09.2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"

7) Приказами Общества в области защиты обработки персональных данных.

8) Инструкцией по обеспечению защиты персональных данных субъектов персональных данных.

9) Политикой конфиденциальности;

10) иными нормативно-правовыми актами Российской Федерации, правовыми документами Оператора.

1.9. В целях противодействия несанкционированного доступа к персональным данным субъектов персональных данных третьими лицами, которые могут осуществить противоправные действия, Инструкция по обеспечению защиты персональных данных субъектов персональных данных, а также иные правовые документы Оператора в части, касающейся защиты персональных данных, описывающих технические и организационные меры защиты и порядок их применения, не подлежат опубликованию в открытых источниках и доступны к изучению и руководству в деятельности только работникам (сотрудникам) Оператора и сотрудникам (должностным лицам) Уполномоченного органа (Роскомнадзора) по запросу.

1.10. Политика размещается на официальном сайте Оператора.

1.11. Оператор гарантирует, что обработка персональных данных (за исключением персональных данных, вводимых лицами в платежных формах, где обработка осуществляется соответственно платежным оператором, платежным агрегатором или иным платежным сервисом), осуществляется на территории Российской Федерации.

Для развертывания сервера Оператора используется платформа VK Cloud, которая размещается в дата-центрах (**ЦОД**) ООО «Цифровое облако».

В VK Cloud зона доступности соответствует отдельному ЦОД уровня Tier III. ЦОД размещены в г. Москве (зоны доступности GZ1, MS1, ME1, PA2).

2. ЦЕЛИ И ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных субъектов персональных данных осуществляется в целях предоставления возможности взаимодействовать с сайтом Оператора для последующего заключения договора (договоров) и последующего их исполнения, участия в партнерской программе для удостоверения личности пользователя в целях недопущения противоправных действий со стороны третьих лиц и выплат вознаграждений пользователям, с целью разработки новых продуктов и услуг и предоставления таких продуктов и услуг, а также информирования об этих услугах.

2.2. Обработка персональных данных осуществляется на основе принципов:

- законности целей и способов обработки персональных данных;

добросовестности;

- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- обеспечения точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных;
- конфиденциальности.

2.3. Пользователь, предоставляющий свои персональные данные Оператору, тем самым соглашается с положениями данной Политики.

3. СБОР ПЕРСОНАЛЬНЫХ ДАННЫХ И СОГЛАСИЕ НА ИХ ОБРАБОТКУ

3.1. Сбор персональных данных Пользователей осуществляется через сайт Оператора, при регистрационных действиях на сайте Оператора, а также при формирования актов при участии пользователей в партнерской программе для выплаты вознаграждений. Сбор Оператором персональных данных может осуществляться при использовании иных услуг Оператора в соответствии с требованиями законодательства Российской Федерации.

3.2. Согласие может быть выражено как в письменной форме, так и в электронной форме путем осуществления определенных действий на сайте Оператора при регистрации или при участии в партнерской программе путем постановки галочки в чекбоксе рядом с графой “Я согласен на обработку моих персональных данных” с сохранением в log-файлах даты и времени дачи согласия.

3.3. На сайте Оператора предусмотрено, что если пользователь не совершит действия, явно направленные на дачу согласия обработки персональных данных, то дальнейшие действия по участию в Партнерской программе (в т.ч. в выводе средств), а также по регистрации и по использованию сервисов Оператора не будут доступны, в связи с тем, что Оператор не вправе обрабатывать персональные данные субъекта, которые необходимы для осуществления целей, предусмотренной настоящей Политикой, без согласия субъекта персональных данных.

4. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Права субъекта персональных данных.

4.1.1. Пользователь имеет право на получение у Оператора информации, касающейся обработки его персональных данных, в том числе объема обрабатываемых персональных данных.

4.1.2. Субъект персональных данных вправе 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.

4.1.3. Субъект персональных данных вправе отозвать согласие на обработку своих персональных данных.

4.1.4. Требование Пользователя составляется в свободной форме в виде письменного документа (в т.ч. в электронной форме), который может быть:

- направлен в адрес Оператора почтовым отправлением;
- направлен на адрес электронной почты documents@salebot.pro;
- направлен в чат с технической поддержкой Оператора.
- иным не запрещенным законодательством Российской Федерации способом.

4.1.5. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях и сообщить об этом не позднее 10 (десяти) рабочих дней с момента получения требования.

4.1.6. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований действующего законодательства или иным образом нарушает его права и свободы, то он вправе обжаловать действия или бездействие Оператора в Уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

4.1.7. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда.

4.2. Обязанности Оператора.

4.2.1. Оператор разъясняет субъекту персональных данных юридические последствия отказа предоставить персональные данные, если это является обязательным в соответствии с законодательством Российской Федерации.

4.2.2. Оператор обязан отвечать на запросы в следующем порядке:

- По факту личного обращения либо при получении письменного запроса Пользователя Оператор, при наличии оснований, обязан в течение 30 дней с даты обращения либо получения запроса предоставить сведения в объеме, установленном действующим законодательством. Такие сведения должны быть представлены в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
- Все обращения регистрируются в Журнале учета обращений субъектов персональных данных по вопросам обработки персональных данных.

4.2.3. Оператор уведомляет субъекта персональных данных об устранении допущенных нарушений

или уничтожении его персональных данных.

4.2.4. В случае получения запроса от уполномоченного органа по защите прав субъектов персональных данных о предоставлении информации, необходимой для осуществления деятельности указанного органа, Оператор обязан сообщить такую информацию в уполномоченный орган в течение 30 дней с даты получения такого запроса или в срок, указанный в запросе.

4.2.5. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

4.2.6. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.3. Оператор обработки персональных данных может выступать в качестве Поверенного по обработке персональных данных для пользователя, оказывающего услуги с использованием программы для ЭВМ (реестр отечественного ПО № 15302) Поверенного (далее – Поручитель).

4.3.1. При оказании услуг Поручитель обязан разрабатывать собственную политику обработки персональных данных с ссылкой на Настоящую политику обработки персональных данных и осуществлять обработку персональных данных только по согласию собственных клиентов Поручителя – субъектов персональных данных. В таком случае Поручитель фактически выступает в качестве Оператора обработки персональных данных для собственных клиентов.

4.3.1.1. Поручитель обязан в собственной политике обработки персональных данных предусмотреть положения, прямо указывающие на Настоящую политику обработки персональных данных, а также положения, разъясняющие порядок дачи собственными клиентами Поручителя согласия на обработку персональных данных Поверенному, порядок обращений к Поверенному по поводу обработки персональных данных и порядок отзыва согласия на обработку Персональных данных Поверенным.

4.3.2. Поручитель – оператор обработки персональных данных – самостоятельно получает у собственных клиентов согласие на обработку персональных данных с ссылкой на Настоящую политику обработки персональных данных, определяет круг данных, которые подвергает обработке, осуществляя указанную обработку в соответствии с требованиями законодательства Российской Федерации.

4.3.3. Данные, фактически обрабатываемые Поручителем – оператором обработки персональных данных –, обрабатываются Поверенным в соответствие с требованиями, установленными Настоящей политикой обработки персональных данных, а также законодательством Российской Федерации, только при наличии соответствующего согласия собственных клиентов Поручителя.

4.3.4. Поверенный гарантирует собственным клиентам Поручителя соблюдение всех установленных требований в соответствии с законодательством Российской Федерации по обработке и защите персональных данных.

4.3.4.1. В случае, если несанкционированный доступ к персональным данным собственных клиентов Поручителя произошел по вине самого Поручителя (например, при разглашении Поручителем конфиденциальной информации, при предоставлении третьим лицам паролей и доступов к защищенным аккаунтам Поручителя, и т.п.), ответственность несет Поручитель самостоятельно.

4.3.5. Собственные клиенты Поручителя – субъекты обработки персональных данных – имеют все права, установленные Настоящей политикой обработки персональных данных, в т.ч. пунктом 4.1. Настоящей политики обработки персональных данных, и законодательством Российской Федерации.

4.3.6. В целях защиты персональных данных клиентов Поручителя – субъектов обработки персональных данных – Поверенный вправе ограничить доступ к аккаунту Поручителя на сервисе Поверенного в случае, если Поручитель не выполняет требования, установленные законодательством Российской Федерации в области обработки и защиты персональных данных и Настоящей политикой обработки персональных данных, и (или) был признан виновным в нарушении требований по обработке персональных данных, до выполнения Поручителем установленных требований и (или) устранению

нарушений в области обработки персональных данных.

4.3.7. Оператор вправе использовать обезличенные и агрегированные данные, полученные в процессе использования Сервисов Пользователями, для анализа, улучшения Сервисов, разработки, обучения и совершенствования моделей искусственного интеллекта, а также запросы пользователей к ИИ-инструментам и ответы системы для повышения качества их работы. Доступ к таким данным предоставляется исключительно уполномоченным администраторам Сервиса.

4.3.7.1. **Оператор гарантирует, что персональные данные пользователей и третьих лиц не используются для обучения и дообучения моделей искусственного интеллекта.** Для указанных целей применяются исключительно обезличенные данные.

5. РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Оператор обеспечивает конфиденциальность и безопасность персональных данных при их обработке в соответствии с требованиями законодательства РФ.

5.2. Оператор не раскрывает третьим лицам и не распространяет персональные данные без согласия на это субъекта персональных данных, если иное не предусмотрено законодательством.

5.3. Работники Оператора, осуществляющие обработку персональных данных, обязаны соблюдать требования регламентирующих документов Оператора в части обеспечения конфиденциальности и безопасности персональных данных.

5.4. Работники Оператора, допущенные к обработке персональных данных, обязаны:

- знать и неукоснительно выполнять положения законодательства Российской Федерации, локальных нормативных и распорядительных актов Оператора, регулирующих вопросы обработки персональных данных; настоящей Политики;
- обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей;
- не разглашать персональные данные, обрабатываемые Оператором;
- сообщать о действиях других лиц, которые могут привести к нарушению положений настоящей Политики;
- сообщать об известных фактах нарушения требований настоящей Политики Ответственному за организацию обработки персональных данных в Организации, назначаемому Приказом Генерального директора Организации.

6. ОБЪЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И УСЛОВИЯ ОБРАБОТКИ

6.1. В целях, указанных в пункте 1.1 настоящей Политики, Оператор обрабатывает следующие категории персональных данных с согласия субъектов персональных данных:

- **Кандидаты на работу – потенциальные работники Оператора:** фамилия, имя, отчество; сведения о документе, удостоверяющем личность; гражданство; адрес прописки; страховой номер индивидуального лицевого счета; платежные реквизиты; сведения о трудовой деятельности; сведения о воинской обязанности; сведения об образовании; номер мобильного телефона; электронная почта.
- **Работники Оператора**: фамилия, имя, отчество; сведения о документе, удостоверяющем личность; гражданство; адрес прописки; страховой номер индивидуального лицевого счета; платежные реквизиты; сведения о трудовой деятельности и реквизиты трудовой книжки; сведения о воинской обязанности; сведения об образовании; номер мобильного телефона; электронная почта.
- **Для пользователей**: фамилия, имя, отчество; мобильный телефон; электронная почта.
- **Лица, участвующие в партнерской программе Оператора (индивидуальные предприниматели и лица, являющиеся плательщиками налога на профессиональный доход):** фамилия, имя, отчество; мобильный телефон; электронная почта; платежные реквизиты; сведения о документе, удостоверяющем личность; сведения о постановке на учет в качестве плательщика налога на профессиональный доход для лиц, имеющие статус плательщика налога на профессиональный доход, или сведения о постановке на учет в качестве индивидуального предпринимателя (номер ОГРНИП и дата постановки) для лиц, зарегистрированных в качестве индивидуальных предпринимателей;
- **Лица, являющиеся представителями (сотрудниками) юридического лица, от имени которого**

осуществляется участие юридического лица в партнерской программе: государственный регистрационный номер о создании юридического лица (ОГРН); фамилия, имя, отчество представителя (сотрудника), от имени которого юридическое лицо осуществляет участие в партнерской программе; должность представителя (сотрудника) юридического лица, от имени которого юридическое лицо осуществляет участие в Партнерской программе; сведения о документе, удостоверяющем личность; мобильный телефон; электронная почта; платежные реквизиты.

- **Потенциальные контрагенты (физические и (или) юридические лица):**
а) для юридических лиц: государственный регистрационный номер о создании юридического лица (ОГРН); фамилия, имя, отчество представителя (сотрудника), от имени которого юридическое лицо осуществляет взаимодействие с Оператором; должность представителя (сотрудника) юридического лица; мобильный телефон; электронная почта; платежные реквизиты;
б) для лиц, имеющих статус индивидуального предпринимателя или статус плательщика налога на профессиональный доход: фамилия, имя, отчество; сведения о постановке на учет в качестве плательщика налога на профессиональный доход для лиц, имеющие статус плательщика налога на профессиональный доход, или сведения о постановке на учет в качестве индивидуального предпринимателя (номер ОГРНИП и дата постановки) для лиц, зарегистрированных в качестве индивидуальных предпринимателей; номер телефона; почта; платежные реквизиты.

- **Исполнители по договорам ГПХ** (физические лица, привлекаемые в качестве исполнителей по договорам, а также кандидаты в исполнители на этапе планирования договора): фамилия, имя, отчество; сведения о документе, удостоверяющем личность; свидетельство о постановке на учет в налоговом органе; электронная почта; мобильный телефон; платежные реквизиты.

- **Работники контрагентов, субподрядчиков, поставщиков и других юридических лиц, имеющих договорные отношения с Оператором**, с которым взаимодействуют работники Оператора в рамках своей деятельности: фамилия, имя, отчество; мобильный телефон; адрес электронной почты.

6.1.1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Оператором не осуществляется.

6.2. Условия обработки персональных данных.

6.2.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Обработка персональных данных субъектов персональных данных без согласия субъекта персональных данных осуществляется только по основаниям и в случаях, прямо предусмотренных законодательством РФ.

6.2.2. Персональные данные могут также включать в себя дополнительно предоставляемые Пользователями данные по запросу Оператора в целях исполнения Оператором обязательств, вытекающих из договоров, заключаемых между Оператором и Пользователем.

6.2.3. Персональные данные могут храниться как на бумажных носителях, так и на электронных носителях.

6.2.4. Персональные данные обрабатываются как с использованием автоматизированных систем, так и без использования автоматизированных систем.

6.2.5. Оператор может использовать персональные данные для отправки важных уведомлений, рекламной и информационной рассылки.

6.2.6. Оператор не передает персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством, и обрабатывает данные субъектов персональных данных самостоятельно.

6.2.7. Персональные данные обрабатывают лично Оператор или только сотрудники Оператора, допущенными Приказом к обработке персональных данных. Работники имеют право обрабатывать только те персональные данные, которые необходимы им для выполнения своих должностных обязанностей. Доступ работников к персональным данным прекращается после прекращения трудовых отношений с работником либо с даты прекращения должностных обязанностей.

6.2.8. Хранение персональных данных субъекта персональных данных осуществляется в форме,

позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных.

6.2.9. Общий срок хранения персональных данных составляет 3 (три) года с момента прекращения договора или иных правоотношений с контрагентами.

6.2.10. Обработка персональных данных Пользователей, осуществляемая без использования средств автоматизации, происходит таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей).

6.2.11. В Обществе обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

6.2.12. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

6.2.13. Серверы располагаются в местах недоступных для лиц, не имеющих доступ к персональным данным Пользователей. Конкретный перечень мер, принимаемых Оператором к хранению персональных данных содержится в соответствующем приказе. Оператор для хранения персональных данных использует базы данных, находящиеся на территории Российской Федерации.

6.2.14. Оператор не осуществляет трансграничную передачу данных субъектов персональных данных.

6.3. Обеспечение безопасности персональных данных.

6.3.1. Оператор обеспечивает безопасность персональных данных, обрабатываемых в информационных системах Оператора, которая достигается путем исключения несанкционированного, в том числе случайного, доступа к ним, а также принятия следующих мер по обеспечению безопасности:

- определение актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах Оператора, необходимых для выполнения требований к защите данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности;
- применение процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы;
- обеспечение работоспособного функционирования компьютерной техники с персональными данными в соответствии с эксплуатационной и технической документацией компьютерной техники и с учетом технических требований информационных систем и средств защиты информации;
- обнаружение и регистрация фактов несанкционированного доступа к персональным данным, несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы и принятие мер;
- восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах Оператора, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах Оператора;
- использование антивирусных средств и средств восстановления системы защиты персональных данных;
- применение средств межсетевого экранирования, в необходимых случаях обнаружения вторжений, анализа защищенности и иных технических средств защиты информации.

6.4. Актуализация, блокирование и уничтожение персональных данных.

6.4.1. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат их актуализации Оператором, а обработка должна быть прекращена.

6.4.2. Пользователь вправе в письменной форме требовать уничтожения своих персональных

данных в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

6.4.3. В случае отсутствия возможности уничтожения персональных данных Оператор осуществляет блокирование таких персональных данных. В случае выявления неправомерной обработки персональных данных при обращении или по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки.

6.4.4. Уничтожение персональных данных осуществляется в течение 30 дней с момента возникновения оснований для уничтожения и путем стирания информации с использованием сертифицированного программного обеспечения с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

6.4.5. Уничтожение документации, содержащей персональные данные осуществляется лично Оператором.

6.5. Прекращение обработки персональных данных.

6.5.1. Условием прекращения обработки персональных данных может являться:

• достижение целей обработки персональных данных;

• истечение срока действия согласия или отзыв согласия субъекта на обработку его персональных данных;

• выявление неправомерной обработки персональных данных

В этом случае персональные данные субъектов уничтожаются в порядке, предусмотренным настоящей Политикой.

7. ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ

7.1. К **организационным мерам защиты персональных данных** относят:

1) издание локальных Актов организации, касающихся обработки персональных данных и их защиты, и ознакомление сотрудников, осуществляющих обработку персональных данных в том объеме и в той мере, который необходим для осуществления трудовой функции и исполнению обязанностей, установленных должностным регламентом.

2) определение объема и перечня персональных данных, которые необходимы для осуществления сотрудниками Организации трудовой функции и обязанностей, установленных должностным регламентом.

3) создание и применение в деятельности организации Политики обработки персональных данных. В свою очередь, Политика обработки персональных данных должна быть в обязательном порядке расположена на сайте Организации в информационно-телекоммуникационной сети “Интернет” (адрес сайта Организации: https://salebot.pro).

4) определение правил доступа и учет доступов к административной части программы для ЭВМ “Сейлбот”.

5) организация проведения проверок на уязвимости программы, где в качестве проверяющих выступают независимые организации (юридические лица).

6) организация мероприятий по поиску и выявлению уязвимостей программы техническими работниками организации, имеющие специализированные знания, навыки и (или) квалификацию в области информационных технологий и (или) информационной безопасности.

7) установление способов профилактики несанкционированного доступа и комплекса мер по предупреждению инцидентов безопасности.

8) проведение мероприятий по обучению сотрудников работе с персональными данными, ознакомление сотрудников с Политикой обработки персональных данных и настоящей инструкцией.

9) информирование пользователей:
- уведомление пользователей программы для ЭВМ “Сейлбот” о необходимости обновления паролей;
- направление рекомендаций к установлению уровня сложности паролей, установлению двухфакторной аутентификации;
- направление предупреждений для пользователей программы для ЭВМ “Сейлбот” об исключении случаев передачи паролей и доступов к собственным аккаунтам программы для ЭВМ “Сейлбот” третьим лицам;
- разработка методических рекомендаций и статей по предупреждению пользователей о возможных угрозах при передаче доступов к аккаунту третьим лицам. Указанные рекомендации и статьи расположены в общем доступе на сайте с документацией в информационно-телекоммуникационной сети “Интернет”.

10) ведение учета кибератак на программу для ЭВМ “Сейлбот”.

11) ведение учета персональных компьютеров и (или) защищенных сервисов, являющиеся таковыми на основании Законодательства Российской Федерации, на которых хранятся персональные данные субъектов персональных данных, ответственным за безопасность и защиту персональных данных.

12) в случае, если в Организации осуществляется хранение персональных данных на бумажных носителях, ответственное лицо обязано вести учет таковым носителям, а также обеспечивать сохранность и безопасность указанных носителей до момента уничтожения бумажных носителей персональных данных субъектов персональных данных, которые уничтожаются в соответствии с требованиями, установленными Законодательством Российской Федерации по хранению персональных данных субъектов персональных данных.

13) проведение инструктажей сотрудников организации по обеспечению защиты и безопасности персональных данных при эксплуатации программы для ЭВМ “Сейлбот”.

14) установление правил и требований для аварийного восстановления системы программы для ЭВМ “Сейлбот”, для резервного копирования системы программы для ЭВМ “Сейлбот”.

15) направление потенциальным кандидатам договора о неразглашении конфиденциальной информации, которая может стать им известной после заключения трудового договора, для осуществления трудовой функции в Организации;

16) обеспечение передачи закрывающих документов (УПД), актов и счетов на оплату, иных платежных поручений и документов, содержащие сведения о персональных данных субъектов персональных данных, а также хранение электронных документов, содержащих персональные данные и переданных на обработку персональных данных, с помощью оператора ЭДО, соответствующее требованиям, установленным Законодательством Российской Федерации.

7.2. Перечисленный в п. 7.1 настоящей Политики перечень организационных мер не является исчерпывающим. Сотрудники Организации, в том числе Генеральный директор, Организации как лицо ответственное за защиту и безопасность персональных данных субъектов персональных данных, вправе принимать и иные организационные меры, которые в должном объеме и степени обеспечивают защиту и безопасность персональных данных субъектов персональных данных.

7.3. К **техническим мерам защиты персональных данных** относят технические средства, программные методы, предназначенные для недопущения несанкционированного доступа (в т.ч. недопущения противоправных действий с персональными данными субъектов) к персональным данным субъектов персональных данных и их защиты, не являющиеся собственной разработкой технических специалистов – разработчиков Организации, а также методы, способы, модели и иные средства, являющиеся собственной разработкой Организации, предназначенные для защиты и безопасности персональных данных.

7.4. К техническим мерам защиты персональных данных относят:

1) фаервол, запрещающий доступ к базе данных извне, – система, которая предотвращает несанкционированный доступ в информационно-телекоммуникационной сети “Интернет”;

1) ограничение доступа средствами аутентификации в базе данных с использованием программных средств и методов;

2) ограничение доступа к серверу средствами ОС Linux, включающая настройку параметров безопасности конфигурационных файлов: пользователей, групп пользователей и процессов с помощью встроенных системных разрешений, групп пользователей;

3) работа с базой данной с использованием ORM;

4) ограничение доступа по IP;

5) разработанная система доступа к аккаунту пользователя – двухфакторная аутентификация;

6) валидация логинов, паролей, адресов электронной почты, вводимых при регистрации и аутентификации;

7) проверка адресов электронной почты на спам с помощью спам-фильтров и на иные подозрительные действия, осуществляемые с данным адресом электронной почты;

8) использование защищенных хостинг сервисов (VK Cloud), в котором обеспечивается:

а) блокирование версии объекта (object lock);

б) шифрование объектов (object storage), обеспечивающее недопущение случайной или преднамеренной публикации содержимого в информационно-телекоммуникационной сети “Интернет”.

в) протокол TLS, обеспечивающее защищенную передачу данных.

г) политика доступа для защищенного управления доступом к ресурсам;

д) установление ключей доступа.

7.4. Перечисленный в п.п. 7.3, 7.4 настоящей Политики перечень технических мер не является исчерпывающим. Сотрудники Организации, в том числе Генеральный директор Организации, как лицо ответственное за защиту и безопасность персональных данных субъектов персональных данных, вправе принимать и иные организационные меры, которые в должном объеме и степени обеспечивают защиту и безопасность персональных данных субъектов персональных данных.

8. ОТВЕТСТВЕННОСТЬ

8.1. Все сотрудники Оператора, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с Политикой, требованиями законодательства РФ.

8.2. Лица, виновные в нарушении требований Политики и законодательства о персональных данных, несут предусмотренную законодательством РФ ответственность.

8.3. Лица, ответственные за обработку персональных данных, назначаются Приказом Генерального директора с начала действия трудовых договоров и до их окончания.