УТВЕРЖДЕНА
Приказом № 6
от 01.03.2021 года

ПОЛИТИКА
о порядке обработки и обеспечения безопасности персональных данных Индивидуального предпринимателя Сидорова Андрея Сергеевича

СОДЕРЖАНИЕ

1. Общие положения.

1.1. Настоящая Политика о порядке обработки и обеспечения безопасности персональных данных (далее – Политика) разработана на основании:

- Федеральный закон № 152 «О защите персональных данных» от 27.07.2006.
- Постановления Правительства РФ №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008.
- Постановление Правительства РФ № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" от 01.11.2012
- Постановление Правительства РФ № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" от 21.03.2012.

1.2. Целями настоящей Политики являются определение обработки и обеспечение безопасности персональных данных.

1.3. В настоящей Политике приведены характеристики процессов обработки персональных данных, осуществляемых Компании, включая:

- цели обработки персональных данных;
- объёмы обрабатываемых персональных данных;
- субъекты, персональные данные которых обрабатываются;
- виды обрабатываемых персональных данных;
- основания обработки персональных данных;
- лица, осуществляющие обработку ПДн.

1.4. Также в настоящей Политике приведены описания мероприятий, выполняемых Компанией в целях:

- соблюдения требований законодательства Российской Федерации в области обработки и защиты персональных данных, а также органов власти, имеющих отношение к регулированию области обработки и защиты персональных данных: Роскомнадзор, ФСБ России, ФСТЭК России;
- обеспечения безопасности обрабатываемых персональных данных;
- соблюдения законных прав субъектов персональных данных.

1.5. Настоящая Политика распространяется на все бизнес процессы компании и обязательна к выполнению всеми подразделениями/сотрудниками Компании.

1.6. В связи с общедоступностью настоящей Политики, более детальное описание процессов обработки и обеспечения безопасности персональных данных описано во внутренних нормативных документах.

2. Определения и термины

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

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

2.3. обработка персональных данных - любое действие (операция) 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;

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

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

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

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

2.8. уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

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

2.11. машинный носитель - магнитный диск, магнитная лента, лазерный диск и иные материальные носители, используемые для записи и хранения информации с помощью электронно-вычислительной техники

2.12. компания – индивидуальный предприниматель Сидоров Андрей Сергеевич (ОГРНИП ОГРНИП 317774600324405 от 07.07.2017г., ИНН 770172770084).

3. Сокращения

ПДн – персональные данные
РФ – Российская Федерация
ФЗ – федеральный закон
НСД – несанкционированный доступ
Закон - Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"

4. Правовые основания и цели обработки ПДн

4.1 Обработка и обеспечение безопасности ПДн Компании осуществляется в соответствии с требованиями Конституции Российской Федерации, Закона, Трудового кодекса Российской Федерации, подзаконных актов, других определяющих случаи и особенности обработки ПДн федеральных законов Российской Федерации, руководящих и методических документов ФСТЭК России и ФСБ России.

4.2 Субъектами ПДн, обрабатываемых Компанией, являются:

- кандидаты на вакантные должности;
- работники Компании, родственники работников Компании, в пределах определяемых законодательством Российской Федерации, если сведения о них предоставляются работником;
- физические лица, с которыми Компанией заключаются договоры гражданско-правового характера;
- представители юридических лиц – контрагентов Компании;
- участники рекламных и маркетинговых мероприятий;
- клиенты – потребители, в т.ч. посетители сайта, принадлежащего Индивидуальному предпринимателю: https://spaonegin.ru/ (далее – «Сайт»);
- физические лица, ПДн которых обрабатываются в интересах третьих лиц – операторов ПДн на основании договора (поручения операторов ПДн).

4.3. Компания осуществляет обработку ПДн субъектов в следующих целях:

- осуществления возложенных на Компанию законодательством Российской Федерации функций, полномочий и обязанностей в соответствии с федеральными законами, в том числе, но не ограничиваясь: Гражданским кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Семейным кодексом Российской Федерации, Федеральным законом от 01.04.1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 28.03.1998 г. № 53-ФЗ «О воинской обязанности и военной службе», Федеральным законом от 26.02.1997 г. № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации», Федеральным законом от 8.02.1998 г. №14-ФЗ «Об обществах с ограниченной ответственностью», Федеральным законом от 07.02.1992 №2300-1 «О защите прав потребителей», Федеральным законом от 21.11.1996 г. № 129-ФЗ «О бухгалтерском учете», Федеральным законом от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», а также операторами ПДн, уставом и локальными актами Компании.

Работников в целях:

- соблюдения трудового, налогового и пенсионного законодательства Российской

Федерации, а именно, но не ограничиваясь: содействия работникам в трудоустройстве, обучении и продвижении по службе, расчета и начисления заработной платы, организация деловых поездок (командировок) работников, оформления доверенностей (в том числе для представления интересов Компании перед третьими лицами), обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества, соблюдения пропускного режима в помещениях Компании, учета рабочего времени, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, а также Уставом и нормативными актами Компании, добровольного страхования жизни, здоровья и/или от несчастных случаев.

Кандидатов на вакантные должности в целях:

- принятия решения о возможности заключения трудового договора с лицами, претендующими на открытые вакансии;

Лиц, входящих в органы управления Компании, не являющихся работниками, в целях:

- выполнения требований, предусмотренных законодательством, в т.ч. обязательное раскрытие информации, аудит, проверка возможности совершения сделок, в том числе сделок с заинтересованностью и/или крупных сделок.

Контрагентов-физических лиц в целях:

- заключения и исполнения договора, одной из сторон которого является физическое лицо;
- рассмотрения возможностей дальнейшего сотрудничества.

Представителей юридических лиц – контрагентов Компании в целях:

- ведения переговоров, заключение и исполнение договоров, по которым предоставляются ПДн работников такого юридического лица для целей исполнения договора по различным направлениям хозяйственной деятельности Компании.

Физических лиц, ПДн которых обрабатываются в интересах третьих лиц – операторов ПДн на основании договора (поручения операторов ПДн) в целях:

- исполнения договоров – поручений операторов ПДн;

Родственников работников Компании в целях:

- исполнения требований законодательства Российской Федерации;
- предоставления дополнительных льгот;
- участия в корпоративных мероприятиях.

Клиентов – потребителей в целях:

- предоставления информации по товарам/услугам, проходящим акциям и специальным предложениям;
- анализа качества предоставляемого Компанией сервиса и улучшению качества обслуживания клиентов Компании.

5. Принципы обработки и обеспечения безопасности ПДн

5.1. Принципы обработки ПДн в Компани:

5.1.1. Обработка ПДн должна осуществляться на законной и справедливой основе.

5.1.2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

5.1.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.

5.1.4. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

5.1.5. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

5.1.6. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2. В Компании используется смешанная обработка ПДн. Под смешанной обработкой понимается автоматизированная и неавтоматизированная обработка ПДн.
5.3. В случае достижения целей обработки ПДн, если другое не предусмотрено законодательством РФ, Компания прекращает обработку и производит уничтожение ПДн. Уничтожение ПДн, в электронном виде, и ПДн, содержащихся на материальных носителях, производится ответственными за этот процесс лицами согласно внутренней документации Компании.
5.4. В Компании используются современные и безопасные технологические решения для автоматизированной обработки, передачи и хранения персональных данных, исключающих несанкционированный доступ и утечку.

6. Основные требования к обработке ПДн

6.1. Обработка ПДн в Компании должна осуществляться с согласия субъекта ПДн кроме случаев, когда такое согласие не требуется или же по поручению, в тех случаях, когда Компания не является оператором ПДн субъектов.
6.2. В случаях предусмотренных законодательством обработка ПДн осуществляется с согласия субъекта ПДн, оформляемого в соответствии со статьей 9 ФЗ №152.
6.3. Рекомендации к порядку получения согласия субъекта ПДн и виду согласия описаны во внутренней документации Компании.
6.4. В Компании ведется учет работников, допущенных к обработке ПДн. Учет ведется в согласованном Перечне лиц допущенных к обработке ПДн.
6.5. Во избежание НСД к ПДн рекомендуется:
6.5.1. При неавтоматизированной обработке руководствоваться требованиями предъявляемыми постановлением Правительства РФ №687 «Об утверждении положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации» от 15.09.2008.
6.5.2. При автоматизированной обработке руководствоваться требованиями предъявляемыми постановлением Правительства РФ №781 «Об утверждении положения об обеспечении безопасности ПДн при их обработке в информационных системах ПДн» от 17.10.2007 и приказом ФСТЭК России №58 "Об утверждении положения о методах и способах защиты информации в информационных системах ПДн".

7. Требования и меры принятые Компанией к защите ПДн

7.1. Компания при обработке ПДн принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного и/или несанкционированного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.
7.2. К таким мерам в соответствии с Законом, в частности, относятся:
- назначение лица, ответственного за организацию обработки ПДн, и лица, ответственного за обеспечение безопасности ПДн;
- разработка и утверждение локальных актов по вопросам обработки и защиты ПДн;
- применение правовых, организационных и технических мер по обеспечению безопасности ПДн: определение угроз безопасности ПДн при их обработке в информационных системах персональных данных, применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн, применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы персональных данных, учет машинных носителей ПДн, если хранение ПДн осуществляется на машинных носителях, обнаружение фактов несанкционированного доступа к Данным и принятие мер по недопущению подобных инцидентов в дальнейшем, восстановление ПДн, модифицированных или уничтоженных вследствие

несанкционированного доступа к ним, установление правил доступа к Данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с Данными в информационной системе персональных данных.

- контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности информационных систем персональных данных;
- оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований Закона, соотношение указанного вреда и принимаемых Компанией мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом;
- соблюдение условий, исключающих несанкционированный доступ к материальным носителям ПДн и обеспечивающих сохранность ПДн;
- ознакомление работников Компании, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами по вопросам обработки и защиты ПДн, и обучение работников Компании.

8. Права и обязанности субъектов ПДн, Компании

8.1.Субъект, Данные которого обрабатываются Компанией, имеет право:

- получать от Компании: подтверждение факта обработки ПДн и сведения о наличии ПДн, относящихся к соответствующему субъекту ПДн; сведения о правовых основаниях и целях обработки ПДн; сведения о применяемых Компанией способах обработки ПДн; сведения о наименовании и местонахождении Компании; сведения о лицах (за исключением работников Компании), которые имеют доступ к Данным или которым могут быть раскрыты ПДн на основании договора с Компанией или на основании федерального закона; перечень обрабатываемых ПДн, относящихся к субъекту ПДн, и информацию об источнике их получения, если иной порядок предоставления таких ПДн не предусмотрен федеральным законом; сведения о сроках обработки ПДн, в том числе о сроках их хранения; сведения о порядке осуществления субъектом ПДн прав, предусмотренных Законом; наименование (Ф.И.О.) и адрес лица, осуществляющего обработку ПДн по поручению Компании; иные сведения, предусмотренные Законом или другими нормативно-правовыми актами Российской Федерации; требовать от Компании уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки; отозвать свое согласие на обработку ПДн в любой момент; требовать устранения неправомерных действий Компании в отношении его ПДн; обжаловать действия или бездействие Компании в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если субъект ПДн считает, что Компания осуществляет обработку его ПДн с нарушением требований Закона или иным образом нарушает его права и свободы; на защиту своих прав и законных интересов, в том числе на возмещения убытков и/или компенсацию морального вреда в судебном порядке.

Сведения, предоставляются субъекту ПДн на основании запроса. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.2. Компания в процессе обработки ПДн обязана:

- предоставлять субъекту ПДн по его запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя;
- разъяснить субъекту ПДн юридические последствия отказа предоставить ПДн, если предоставление ПДн является обязательным в соответствии с федеральным законом;
- до начала обработки ПДн (если ПДн получены не от субъекта ПДн) предоставить субъекту ПДн следующую информацию, за исключением случаев, предусмотренных частью 4 статьи 18 Закона:

1) наименование либо фамилия, имя, отчество и адрес Компании или ее представителя;
2) цель обработки ПДн и ее правовое основание;
3) предполагаемые пользователи ПДн;
4) установленные Законом права субъектов ПДн;
5) источник получения ПДн.

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;
- опубликовать в сети Интернет и обеспечить неограниченный доступ с использованием сети Интернет к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- предоставить субъектам ПДн и/или их представителям безвозмездно возможность ознакомления с Данными при обращении с соответствующим запросом в течение 30 дней с даты получения подобного запроса;
- осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) с момента обращения или получения запроса на период проверки, в случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекту ПДн или его представителя либо уполномоченного органа по защите прав субъектов персональных данных;
- уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) в течение 7 рабочих дней со дня представления сведений и снять блокирование ПДн, в случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн или его представителем;
- прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Компании, в случае выявления неправомерной обработки ПДн, осуществляемой Компанией или лицом, действующим на основании договора с Компанией, в срок, не превышающий 3 рабочих дней с даты этого выявления;
- прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по договору с Компанией) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по договору с Компанией) по достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, в случае достижения цели обработки ПДн;
- прекратить обработку ПДн или обеспечить ее прекращение и уничтожить ПДн или обеспечить их уничтожение в случае отзыва субъектом ПДн согласия на обработку ПДн, если Компания не вправе осуществлять обработку ПДн без согласия субъекта ПДн.

9. Обязанности сотрудников Компании

9.1. Работники Компании, допущенные к обработке ПДн, обязаны:
9.1.1. Ознакомиться с данной Политикой и внутренними документами, регламентирующими процесс обработки ПДн, и выполнять требования этих документов.
9.1.2. Обрабатывать ПДн только в рамках выполнения своих должностных обязанностей.
9.1.3. Не разглашать ПДн, к которым был получен доступ в рамках исполнения своих трудовых обязанностей
9.1.4. Информировать о фактах разглашения (уничтожения, искажения) ПДн Уполномоченных сотрудников.

10. Сроки обработки (хранения) ПДн

10.1. Сроки обработки (хранения) ПДн определяются исходя из целей обработки ПДн, в соответствии со сроком действия договора с субъектом ПДн, требованиями федеральных законов, требованиями операторов ПДн, по поручению которых Компания осуществляет обработку ПДн,

основными правилами работы архивов организаций, сроками исковой давности.
10.2. ПДн, срок обработки (хранения) которых истек, должны быть уничтожены, если иное не предусмотрено федеральным законом. Хранение ПДн после прекращения их обработки допускается только после их обезличивания.

11. Порядок получения разъяснений по вопросам обработки ПДн

11.1. Лица, чьи ПДн обрабатываются Компанией, могут получить разъяснения по вопросам обработки своих ПДн, обратившись лично в Компанию или направив соответствующий письменный запрос по адресу местонахождения Компании:
г. Москва, ул. Малая Полянка, д. 2
11.2. В случае направления официального запроса в Компанию в тексте запроса необходимо указать:
- фамилию, имя, отчество субъекта ПДн или его представителя;
- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие наличие у субъекта ПДн отношений с Компанией;
- информацию для обратной связи с целью направления Компанией ответа на запрос;
- подпись субъекта ПДн (или его представителя). Если запрос отправляется в электронном виде, то он должен быть оформлен в виде электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

12. Заключительные положения

Настоящая Политика является локальным нормативным актом Компании. Настоящая Политика является общедоступной. Общедоступность настоящей Политики обеспечивается публикацией на Сайте Компании.
Настоящая Политика может быть пересмотрена в любом из следующих случаев:
- при изменении законодательства Российской Федерации в области обработки и защиты персональных данных;
- в случаях получения предписаний от компетентных государственных органов на устранение несоответствий, затрагивающих область действия Политики;

Компания имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.