Приложение к Приказу № Пр-20171114-4 от 14.11.2017

УТВЕРЖДАЮ

Генеральный директор
ООО УК «ОТКРЫТИЕ»

_____ В.В. Денисова

«14» ноября 2017 г.

ПОЛИТИКА
ООО УК «ОТКРЫТИЕ» в отношении обработки персональных данных

Москва, 2017

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика Общества с ограниченной ответственностью «Управляющая компания «ОТКРЫТИЕ» в отношении обработки персональных данных (далее – Политика) определяет принципы, цели и условия обработки персональных данных (ПДн), права субъектов ПДн, а также основные механизмы их защиты в Обществе с ограниченной ответственностью «Управляющая компания «ОТКРЫТИЕ» (далее – Общество). При организации и осуществлении обработки ПДн Общество руководствуется положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также принятыми в соответствии с ним нормативно-правовыми актами.

Настоящая Политика является основным руководящим внутренним документом Общества, определяющим требования, предъявляемые в отношении обработки и обеспечения безопасности ПДн.

Настоящая Политика разработана в целях реализации положений законодательства Российской Федерации в отношении обработки ПДн, а также требований нормативных и методических документов по защите ПДн.

Настоящая Политика разработана в соответствии с положениями действующих нормативно-правовых актов Российской Федерации, в том числе:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»);
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Требования настоящей Политики обязательны для всех структурных подразделений и должностных лиц Общества.

1.1. Принципы обработки персональных данных Обществом

Обработка ПДн Обществом осуществляется на основе принципов:

- законности и справедливости целей и способов обработки ПДн;
- соответствия целей обработки ПДн законным целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Общества;
- соответствия объема и содержания обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- точности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимости между собой целей баз данных, содержащих ПДн;
- хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, или устанавливающий срок хранения федеральный закон, договор, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.
- уничтожения ПДн по достижении целей их обработки, в случае утраты необходимости в достижении целей обработки или по окончании срока хранения ПДн, установленного федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

Обработка ПДн Обществом осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления, доступа), обезличивания, блокирования, удаления, уничтожения.

1.2. Цели и условия обработки персональных данных Обществом

Обработка ПДн Обществом осуществляется на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей. Обработке подлежат только ПДн, которые отвечают целям их обработки. Содержание и объем обрабатываемых Обществом ПДн соответствует заявленным целям обработки.

Общество осуществляет обработку ПДн в следующих целях:

- заключения и исполнения договоров доверительного управления активами в соответствии с имеющимися у Общества Лицензиями ФСФР России, а также уставом и внутренними документами Общества;
- формирования Обществом клиентской истории для более качественного оказания услуг;
- организации кадрового, налогового учета, учета плательщиков страховых взносов для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия в трудоустройстве, обучении, работе и продвижению по службе, пользовании различного вида льготами, обеспечении личной безопасности, контроля количества и качества выполняемой работы сотрудниками Общества;
- в целях соблюдения Федерального закона № 173-ФЗ от 28.06.2014 «Об особенностях осуществления финансовых операций с иностранными гражданами и юридическими лицами, о внесении изменений в Кодекс Российской Федерации об административных правонарушениях и признании утратившими силу отдельных положений законодательных актов Российской Федерации», иных нормативных правовых актов, требований FATCA, заключения/исполнения/содействия исполнению договора, или рассмотрения вопроса о возможности заключения договора, осуществления прав и законных интересов либо для достижения общественно значимых целей, в целях создания/повышения качества/продвижения товаров, работ, услуг на рынке;
- исполнения обязанностей, предусмотренных законодательством Российской Федерации, в частности Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

1.3. Состав и субъекты персональных данных, обрабатываемых Обществом

Общество обрабатывает ПДн следующих субъектов ПДн:

- физических лиц, ПДн которых были получены в рамках заключенных Обществом договоров доверительного управления;
- физических лиц, состоящих/ранее состоявших/планирующих вступить с Обществом в трудовые отношения.

Общество осуществляет обработку следующих ПДн: фамилия, имя, отчество, дата рождения, паспортные данные, пол, номер ИНН, гражданство, адрес места жительства, номера телефонов, номер страхового свидетельства обязательного пенсионного страхования, сведения о семейном положении, сведения об образования, сведения о трудовой деятельности, а также иные сведения, необходимые Обществу для реализации целей обработки ПДн. Полный состав ПДн определяется Перечнем персональных данных, обрабатываемых в ООО УК «ОТКРЫТИЕ», утверждаемым генеральным директором Общества.

Общество не осуществляет обработку специальных категорий ПДн, в том числе данных субъекта ПДн о его политических, религиозных и иных убеждениях, частной жизни, членстве в различных объединениях, профессиональных союзах.

1.4. Согласие на обработку персональных данных

Получение и обработка ПДн в случаях, предусмотренных ФЗ «О персональных данных», осуществляется Обществом с письменного согласия субъекта ПДн.

Письменное согласие субъекта ПДн должно включать:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Общества;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Обществом способов обработки ПДн;
- срок, в течение которого действует согласие, а также порядок его отзыва;
- подпись субъекта ПДн.

Типовые формы согласий на обработку ПДн утверждаются приказом Генеральным директором Общества.

Субъект ПДн дает Обществу согласие на обработку своих ПДн свободно, в своей воле и своем интересе. Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления в Общество письменного заявления в свободной форме. В этом случае Общество обязуется прекратить обработку, а также уничтожить все имеющиеся в Обществе ПДн в сроки, установленные ФЗ «О персональных данных».

Общество вправе обрабатывать ПДн без согласия субъекта ПДн (или при отзыве субъектом ПДн указанного согласия) при наличии оснований, указанных в ФЗ «О персональных данных».

Общество вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этой стороной договора (поручения на обработку ПДн). Лицо, осуществляющее обработку ПДн по поручению Общества, обязано соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ «О персональных данных».

Передача ПДн третьим лицам осуществляется Обществом с согласия субъекта ПДн в соответствии с требованиями действующего законодательства.

1.5. Трансграничная передача персональных данных

Общество не осуществляет трансграничную передачу ПДн.

1.6. Период обработки и хранения персональных данных

Срок обработки ПДн определяется в соответствии со сроком действия договора с субъектом ПДн, сроком исковой давности, Приказом Минкультуры Российской Федерации от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», сроком исковой давности, а также иными требованиями законодательства Российской Федерации.

Обработка ПДн начинается – с момента поступления в Общество и прекращается:

- в случае выявления неправомерных действий с ПДн в срок, не превышающий трех рабочих дней с даты такого выявления, Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Общество в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Общество уведомляет субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены Роскомнадзором - также этот орган;

– в случае достижения цели обработки ПДн Общество незамедлительно прекращает обработку ПДн и уничтожает соответствующие ПДн в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки ПДн;

– в случае отзыва субъектом ПДн согласия на обработку своих ПДн Общество прекращает обработку ПДн и уничтожает (за исключением ПДн, которые хранятся в соответствии с действующим законодательством) ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва. Об уничтожении ПДн Общество уведомляет субъекта ПДн.

Уничтожение ПДн производится в случаях и в сроки, указанные выше, за исключением ПДн бухгалтерского и кадрового учета, которые хранятся в соответствии с действующим законодательством Российской Федерации.

1.7. Права субъектов персональных данных

Субъект ПДн имеет право на получение информации, касающейся обработки Обществом его ПДн, в том числе содержащей:

– подтверждение факта обработки ПДн Обществом;
– правовые основания и цели обработки ПДн;
– цели и применяемые Обществом способы обработки ПДн;
– наименование и местонахождение Общества, сведения о лицах (за исключением сотрудников Общества), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Обществом или на основании федерального закона;
– обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
– сроки обработки ПДн, в том числе сроки их хранения;
– порядок осуществления субъектов ПДн прав, предусмотренных ФЗ «О персональных данных»;
– информацию об осуществленной или о предполагаемой трансграничной передаче данных;
– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Общества, если обработка поручена или будет поручена такому лицу;
– иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

Общество предоставляет указанную информацию на основании соответствующего письменного заявления субъекта ПДн (далее – Заявление), поданного в головном офисе Общества по адресу: г. Москва, ул. Кожевническая, д.14, стр. 5 или направленного на почтовый адрес Общества: г. Москва, ул. Кожевническая, д.14, стр. 5. Заявление должно содержать номер основного документа, удостоверяющего личность субъекта ПДн, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн обществом, подпись субъекта ПДн. Общество обязуется сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн в течение тридцати дней с даты получения Заявления субъекта ПДн.

Субъект ПДн вправе требовать от Общества уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Если субъект ПДн считает, что Общество осуществляет обработку его ПДн с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

1.8. Обеспечение безопасности персональных данных

Общество принимает необходимые и достаточные правовые, организационные и технические меры для обеспечения безопасности ПДн от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий. Необходимость и достаточность применяемых мер и средств определяется Обществом в соответствии с требованиями законодательства Российской Федерации в области обработки ПДн.

Общество не несет ответственности, если ПДн стали известны неограниченному кругу лиц по вине самого субъекта ПДн.

В целях координации действий по выполнению требований законодательства Российской Федерации в области обработки ПДн в Обществе назначены лица, ответственные за организацию обработки и обеспечение безопасности ПДн.

Общество проводит ознакомление сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации в отношении обработки ПДн, в том числе требованиями к защите ПДн, внутренними документами Общества в отношении обработки ПДн.

1.9. Оценка вреда

Возможный вред, причиняемый субъекту ПДн в случае нарушения безопасности ПДн в ИСПДн, в соответствии с Частной моделью угроз безопасности персональных данных при их обработке в информационной системе персональных данных ООО УК «ОТКРЫТИЕ» определяется как незначительный в виду как целей обработки ПДн, так и в соотношении с принимаемыми мерами.

2. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Организационная структура

Структуру, обеспечивающую обработку и защиту ПДн, составляют:

- ответственный работник за организацию обработки ПДн;
- ответственный работник за обеспечение безопасности ПДн;
- подразделения и работники, осуществляющие непосредственную обработку ПДн;
- система защиты ПДн, обеспечивающая защиту ПДн от угроз информационной безопасности.

Ответственный работник за организацию обработки ПДн отвечает за реализацию следующих мероприятий:

- методологическое обеспечение безопасности ПДн;
- контроль выполнения мероприятий по защите ПДн;
- мониторинг изменений в законодательстве Российской Федерации в отношении обработки ПДн;
- организацию приема и обработки обращений и запросов субъектов ПДн.
- мониторинг планируемых изменений в системе обработки ПДн и/или системе защиты ПДн.
- контроль получения согласий субъектов ПДн на обработку ПДн, предоставления субъектам ПДн доступа к своим ПДн, реагирования на обращения субъектов ПДн и Роскомнадзора.

Ответственный работник за обеспечение безопасности ПДн:

- проведение мероприятий по организации обеспечения безопасности ПДн;
- проведение мероприятий по техническому обеспечению безопасности ПДн при их обработке в информационных системах персональных данных;
- контроль соблюдения работниками, обрабатывающими персональные данные, правил обеспечения безопасности персональных данных;

Доступ работников к ПДн может предоставляться исключительно в рамках выполнения должностных обязанностей, ровно в том объеме, в котором они необходимы для работы.

2.2. Порядок обработки обращений субъектов персональных данных

Ответственный работник за организацию обработки ПДн осуществляет контроль обработки обращений субъектов ПДн.

При поступлении обращения от субъекта ПДн Ответственный работник за организацию обработки ПДн обязан проконтролировать:

- регистрацию запроса;
- уведомление руководство Общества о поступлении обращения субъекта ПДн;
- подготовку подразделениями Общества ответа, удовлетворяющего запрос субъекта ПДн, или мотивированного отказа в случае неправомерности запроса;
- направление соответствующего ответ в адрес субъекта ПДн в сроки, определенные ФЗ «О персональных данных». Подготовка и отправка ответа осуществляются безвозмездно для субъекта ПДн.

Ответственный работник за организацию обработки ПДн должен сделать соответствующую запись в Журнале учета обращений субъектов ПДн. Журнал утверждается Генеральным директором Общества.

2.3. Порядок уничтожения персональных данных

Ответственный работник за организацию обработки ПДн осуществляет контроль выполнения работ по уничтожению ПДн.

Уничтожение ПДн проводится комиссией, назначаемой приказом Генерального директора Общества. Председателем комиссии является Ответственный за обработку ПДн, который осуществляет контроль необходимости и организацию уничтожения ПДн.

При наступлении любого из событий, повлекших необходимость уничтожения ПДн, Ответственный работник за организацию обработки ПДн обязан:

- Уведомить членов комиссии о работах по уничтожению ПДн, определить время и место работы комиссии;
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся ПДн подлежащие уничтожению (и/или материальные носители ПДн);
- определить технологию (приём, способ) уничтожения ПДн (и/или материальных носителей ПДн), определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение ПДн;
- произвести уничтожение ПДн (и/или материальных носителей ПДн);
- оформить соответствующий Акт об уничтожении ПДн (и/или материальных носителей ПДн);
- в случае необходимости уведомить об уничтожении ПДн субъекта ПДн и/или Роскомнадзор.

2.4. Порядок хранения материальных носителей персональных данных

Основные принципы хранения материальных носителей ПДн:

- при фиксации ПДн на материальных носителях не допускать фиксацию на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;
- при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Хранение материальных носителей ПДн осуществляется на основании соответствующего приказа Генерального директора Общества.

2.5. Доступ в помещения обработки персональных данных

Доступ в помещения, в которых размещаются средства обработки и/или защиты ПДн, разрешен только работникам Общества в соответствии с их должностными обязанностями.

Доступ в указанные помещения посетителям Общества разрешается только в сопровождении работников Общества по разовым пропускам.

3. ТЕХНИЧЕСКАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Общие положения

Основными целями обеспечения безопасности ПДн являются:

- предотвращение нарушений прав субъекта ПДн при обработке его ПДн;
- предотвращение утечки, несанкционированного искажения или блокирования ПДн.

Для защиты ПДн, обрабатываемых в Обществе, внедрена система защиты ПДн – комплексная система, позволяющая обеспечить конфиденциальность, целостность и доступность ПДн, обрабатываемых в Обществе.

Обоснование комплекса мероприятий по обеспечению безопасности ПДн в Обществе производится с учетом результатов оценки опасности угроз и определения уровня защищенности ПДн в соответствии с Постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Общество не несет ответственности, если ПДн стали известны неограниченному кругу лиц по вине самого субъекта ПДн.

3.2. Состав системы защиты персональных данных

Система защиты ПДн в Обществе реализует следующие меры по обеспечению безопасности ПДн:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрация событий безопасности;
- антивирусная защита;
- контроль (анализ) защищенности ПДн;
- защита технических средств;
- защита информационных систем, ее средств, систем связи и передачи данных.

3.3. Требования к системе защиты персональных данных

Система защиты ПДн в Обществе должна обеспечивать:

- межсетевое экранирование между сетью Общества и внешними сетями, с которыми происходит информационное взаимодействие (разрешенными для взаимодействия могут быть только адреса и порты, необходимые для выполнения бизнес-процессов, процессов их сопровождающих);
- антивирусную защиту рабочих станций и серверов;
- однофакторную (пароль) аутентификацию при локальном доступе в сеть Общества, двухфакторную аутентификацию при удаленном доступе,
- соответствие паролей требованиям парольных политик;
- разграничение доступа средствами операционных систем, систем управления базами данных и прикладного программного к ПДн;
- фиксацию подсистемой регистрации событий фактов доступа работников к ПДн.
- защиту ПДн от НСД при передаче по внешним каналам связи, путем шифрования передаваемых данных либо с использованием технологии VPN, аналогично (путем шифрования) должен быть ограничен доступ к ПДн в том случае, если они станут размещаться на съемных носителях информации или на мобильных устройствах (например, ноутбуках).
- доступность ПДн путем резервирования элементов информационных систем ПДн.

В целях защиты ПДн от разглашения или утечки, должны быть использованы системы предотвращения утечки информации, категорирования сайтов и разграничения доступа к сети Интернет.

Доступ к съемным носителям информации, возможности отправки писем на внешние почтовые серверы по умолчанию должен отсутствовать и предоставляться только в рамках исполнения должностных обязанностей, при этом должен вестись регулярный контроль использования почты, сети Интернет, съемных носителей (передаваемой и копируемой информации).

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящая Политика является публичным, равнодоступным документом и предоставляется для ознакомления неограниченному кругу лиц на официальном сайте Общества по адресу: www.open-am.ru.

В настоящую Политику могут быть внесены изменения, дополнения в следующих случаях:

- изменения целей и условий, системы защиты обработки ПДн;
- изменения законодательства в области обработки ПДн и защиты прав субъектов ПДн.

Все изменения и дополнения в Политику утверждаются генеральным директором Общества и подлежат опубликованию в соответствующем порядке.

Все сотрудники Общества подлежат обязательному ознакомлению с настоящей Политикой и несут предусмотренную законодательством Российской Федерации ответственность за нарушение её положений.