

Политика конфиденциальности

1. Общие положения

1.1. Настоящая Политика регламентирует организацию деятельности ООО «МД Сервис» (115191, г. Москва, Муниципальный округ Даниловский вн.тер.г., ул. Большая Тульская, д. 10, стр. 38, пом. 1/П, ОГРН: 1187746514108, ИНН: 7704455889, КПП: 772501001) (далее – Оператор персональных данных), в отношении обработки персональных данных, полученных Оператором персональных данных в соответствии с п. 1.7. настоящей Политики, цели и принципы обработки указанных персональных данных Оператором обработки персональных данных.

1.2. Настоящая Политика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

1.3. В настоящей Политике используются основные понятия и условные обозначения в соответствии с Федеральным законом «О персональных данных».

1.4. Оператор персональных данных организует и обеспечивает обработку персональных данных и безопасность персональных данных при обработке в соответствии с требованиями Федерального закона «О персональных данных» и нормативных правовых актов Российской Федерации.

1.5. Настоящая Политика устанавливает обязательства Оператора персональных данных по неразглашению и обеспечению конфиденциальности персональных данных собственников недвижимого имущества, расположенного в многоквартирных домах находящихся под управлением Оператора персональных данных (далее – пользователь).

1.6. Персональные данные, разрешенные к обработке в рамках настоящей Политики, включают в себя следующую информацию: фамилия, имя, отчество, дата рождения, место рождения, адрес регистрации и фактическое место жительства, данные паспорта (серия, номер, дата выдачи, орган, выдавший документ, страховой номер индивидуального лицевого счёта, гражданство, сведения об объектах недвижимости, принадлежащих на праве собственности (или ином праве), пол, идентификационный номер налогоплательщика, данные о льготах (инвалидность, ветеран, многодетная семья, участник ВОВ, вдова/вдовец), адрес электронной почты, номер телефона, другие персональные данные необходимые для достижения цели обработки персональных данных.

1.7. Пользователь дистанционно предоставляет Оператору персональных данных свои персональные данные, кроме того персональные данные могут быть предоставлены Оператору персональных данных путем заполнения форм и анкет, а также свободно, своей волей и в своем интересе дает согласие Оператору персональных данных на обработку своих персональных данных.

Такое согласие вступает в силу со дня предоставления Оператору персональных данных и действует в течение неопределенного срока и может быть отозвано по письменному заявлению, направленному заказным (ценным) письмом с описью вложения и уведомлением о вручении Оператору персональных данных.

1.8. Персональные данные пользователей обрабатываются автоматизированным и без использования средств автоматизации способами.

2. Цели обработки персональных данных

2.1. Оператор персональных данных обрабатывает персональные данные в следующих целях: проведение общего собрания собственников помещений в многоквартирном доме, заключение и исполнение договора управления многоквартирным домом, ведение реестра собственников помещений в соответствии с ЖК РФ.

3. Сроки обработки персональных данных

3.1. Срок обработки персональных данных пользователей, определяется организационно-распорядительными документами Оператора персональных данных в соответствии с положениями Федерального закона «О персональных данных».

Сроки обработки персональных данных пользователей определяются в соответствии со сроком действия договора управления многоквартирным домом, сроками исковой давности, а также иными сроками, установленными законодательством РФ и организационно-распорядительными документами Оператора персональных данных.

4. Принципы и условия обработки персональных данных

4.1. Обработка персональных данных Оператором персональных данных осуществляется на основе следующих принципов:

4.1.1. законность и справедливость обработки персональных данных;

4.1.2. ограничение обработки персональных данных при достижении заранее определенных и конкретных целей обработки. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

4.1.3. недопустимость объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

4.1.4. обработке подлежат только персональные данные, которые отвечают целям их обработки;

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

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

4.1.7. хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Уничтожение персональных данных либо обезличивание по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

4.1.8. соблюдение конфиденциальности персональных данных;

4.1.9. наличие согласия субъекта персональных данных на обработку его персональных данных.

5. Меры по обеспечению защиты персональных данных

5.1. В соответствии с частью 2 статьи 19 Федерального закона «О персональных данных» для обеспечения безопасности персональных данных при их обработке Оператором персональных данных применяются организационные и технические меры защиты.

5.2. Оператор персональных данных определяет тип угроз безопасности и уровень защищенности персональных данных, которые хранятся в информационных системах, и предпринимает меры по защите информации.

5.2.1. Угрозы защищенности персональных данных

Угрозы 1-го типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

Угрозы 2-го типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

Угрозы 3-го типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

5.2.2. Уровни защищенности (УЗ) персональных данных

УЗ-1 устанавливается:

если существуют угрозы I типа и информсистема работает со специальными, биометрическими или иными категориями ПД;

если существуют угрозы II типа и информсистема работает со специальными категориями ПД свыше 100 тысяч граждан.

УЗ-2 устанавливается при угрозах типов:

I и работе с общедоступными личными данными;

II и работе с личными данными служащих оператора или при работе со специальной категорией ниже 100 тысяч человек;

II и работе с использованием биометрических личных данных;

II и обработке общедоступных личных данных при количестве от 100 тысяч человек (без персонала оператора);

II и работе с другими видами ПД с количеством от 100 тысяч человек (без учета работников оператора);

III и работе со специальной категорией более чем 100 тысяч человек (не считая персонала оператора).

УЗ-3 устанавливается при наличии угроз следующих типов:

II, включая работу с ПД общедоступного характера с количеством людей до 100 тысяч человек;

II с работой с другими категориями до 100 тысяч человек;

III с обработкой специальных категорий до 100 тысяч человек;

III с использованием биометрических ПД;

III с работой с другими категориями, превышающими 100 тысяч человек (кроме персонала оператора).

УЗ-4 устанавливается при угрозах:

III типа и работе с общедоступной информацией;

III типа и обработке других категорий меньше 100 тысяч человек. 2.2.

5.3. При 4-м уровне защищенности персональных данных Оператор персональных данных:

— обеспечивает режим безопасности помещений, в которых размещает информационную систему;

— обеспечивает сохранность носителей информации;

— утверждает перечень работников, допущенных до персональных данных;

— использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

5.4. При 3-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пункте 5.3. настоящей Политики, Оператор персональных данных назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

5.5. При 2-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пунктах 5.3 и 5.4 настоящей Политики, Оператор персональных данных ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

5.6. При 1-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пунктах 5.3.-5.5. настоящей Политики, Оператор персональных данных:

— обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к персональным данным в системе;

— создает отдел, ответственный за безопасность персональных данных в системе, либо возлагает такую обязанность на один из существующих отделов Оператора персональных данных.

5.7. В целях защиты персональных данных на бумажных носителях Оператор персональных данных:

— приказом назначает ответственного за обработку персональных данных;

— ограничивает допуск в помещения, где хранятся документы, которые содержат персональные данные;

— хранит документы, содержащие персональные данные в шкафах, запирающихся на ключ.

5.8. Работники, допущенные к персональным данным, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных не допускаются.

5.9. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия субъекта персональных данных на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных. Передача информации, содержащей сведения о персональных данных, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

6. Права и обязанности в области защиты персональных данных

6.1. Оператор персональных данных обязан:

6.1.1. Использовать полученную информацию исключительно для целей, указанных в п. 2 настоящей Политики.

6.1.2. Обеспечить конфиденциальность полученных персональных данных, не разглашать их без предварительного разрешения субъекта персональных данных, а также не осуществлять продажу, обмен, опубликование, либо разглашение иными возможными способами переданных персональных данных.

6.1.3. Принимать необходимые и достаточные меры для защиты персональных данных.

6.1.4. Осуществить блокирование/уничтожение персональных данных, относящихся к соответствующему пользователю, с момента обращения или запроса пользователя или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных на период проверки, в том числе в случае выявления недостоверных персональных данных или неправомерных действий.

6.2. Субъект персональных данных, предоставляющий Оператору персональных данных право обработки своих персональных данных, имеет право на доступ к своим персональным данным и право на получение информации, касающейся обработки его персональных данных в соответствии со статьей 14 Федерального закона «О персональных данных».

6.3. При достижении целей обработки и после истечения срока нормативного хранения, или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, персональные данные пользователя в электронном виде и документы содержащие персональные данные пользователя подлежат уничтожению. Для этого Оператор персональных данных создает комиссию и проводит экспертизу ценности документов. В ходе проведения экспертизы комиссия отбирает документы с истекшими сроками хранения и по итогам отбора составляет акт о выделении к уничтожению документов, не подлежащих хранению. После чего документы измельчаются в шредере. Персональные данные пользователей в электронном виде стираются с информационных носителей, либо физически уничтожаются сами носители, на которых хранится информация. Факт уничтожения персональных данных оформляется актом.

7. Ответственность в области защиты персональных данных

7.1. Оператор персональных данных и его работники несут ответственность за нарушение положений настоящей Политики и норм, регулирующих обработку персональных данных и безопасность персональных данных при их обработке.

8. Дополнительные условия

8.1. Оператор персональных данных вправе вносить изменения в настоящую Политику конфиденциальности без согласия пользователя.

8.2. Новая Политика вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики.