

Политика обработки персональных данных

Общие положения

Настоящая политика разработана в соответствии с Федеральным законом РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных», иным российским законодательством, регулирующим сферу защиты и обработки персональных данных.

Управляющая компания берет на себя обязательство соблюдать права физических лиц, чьим персональным данным она оперирует, обеспечивая их сохранность и защищенность от несанкционированного доступа посторонних лиц.

Термины и определения

Используемые термины определены следующим образом:

- **Персональные данные** — любые сведения, прямо или косвенно идентифицирующие физическое лицо (субъекта персональных данных);
- **Обработка персональных данных** — операции, осуществляемые с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, использование, передачу, обезличивание, блокировку, удаление, уничтожение данных;
- **Субъекты персональных данных** — физические лица, персональные данные которых обрабатываются управляющей компанией (собственники, наниматели жилых помещений в многоквартирных домах, заключившие договоры на обслуживание; лица, зарегистрированные по месту жительства/пребывания в жилых помещениях многоквартирных владельцы жилья, арендаторы, сотрудники, партнеры, клиенты и другие заинтересованные лица);
- **Оператор** — управляющая компания, выполняющая функции обработки персональных данных.

Цель обработки персональных данных

Основная цель обработки персональных данных заключается в надлежащем управлении жилым фондом, управление комплексом недвижимого имущества в многоквартирном доме, обеспечение эксплуатации комплекса недвижимого имущества в многоквартирном доме, оказание услуг в сфере жилищно-коммунального хозяйства в многоквартирном доме, выполнении обязательств перед владельцами недвижимости и жильцами, исполнении заключенных договоров, взаимодействии с государственными структурами и соблюдением российского законодательства.

Целями также являются:

- управление общим имуществом многоквартирных домов;
- оказание жилищно-коммунальных услуг;
- оказание дополнительных услуг;
- ведение учета платежей и расчеты по обслуживанию недвижимости;
- контроль качества предоставленных услуг;
- защита договорных интересов участников правоотношений;
- реализация полномочий в области контроля над использованием и сохранением общедомового имущества.

Основание обработки персональных данных

Юридическим основанием обработки персональных данных выступают:

- Федеральный закон № 152-ФЗ «О персональных данных»;
- Гражданский кодекс РФ;
- Жилищный кодекс РФ;
- Трудовой кодекс РФ;
- Договоры с субъектами персональных данных;
- Подзаконные акты федеральных органов власти и местных администраций.

Классификация субъектов персональных данных

Категории субъектов персональных данных включают:

- владельцев жилой недвижимости;
- пользователей и нанимателей жилых помещений;
- работников управляющей компании;
- поставщиков товаров и услуг;
- иных третьих лиц, участвующих в деятельности организации.

Состав обрабатываемых персональных данных

Перечень обрабатываемой информации содержит:

- фамилию, имя, отчество;
- место жительства/регистрации;
- контактные телефоны и электронную почту;
- паспортные данные или иной документ, подтверждающий личность;
- идентификационный номер налогоплательщика (ИНН), СНИЛС, банковские реквизиты;
- сведения о правах собственности на имущество (жилое помещение, доля владения);
- информацию об оказании услуг и проведенных платежах;
- фотографии и видеоматериалы с камер наблюдения: система видеонаблюдения используется исключительно в целях обеспечения охраны и безопасности объектов, принадлежащих управляющей компании, и предназначена для фиксации визуальной обстановки без автоматического распознавания индивидуальных признаков физического лица (лиц) и последующей автоматической обработки полученной информации. Запись изображений производится без возможности автоматизированного извлечения персональных данных, включая идентификационные признаки, такие как черты лица, и не предполагает дальнейшего анализа биометрической информации. Использование системы видеонаблюдения ограничено указанными целями и не подразумевает сбор и обработку специальных категорий персональных данных.);
- биометрические данные

Средства обеспечения безопасности персональных данных

Для защиты персональных данных от незаконного вмешательства управляющая компания применяет комплекс организационных и технических мер, включающих:

- ограничение доступа персонала к конфиденциальной информации;
- применение сертифицированного оборудования и программного обеспечения;
- регулярную проверку соответствия используемых средств требованиям безопасности;
- шифрование передаваемой информации;
- периодическое проведение аудита мер защиты.

Условия передачи персональных данных третьим лицам

Передача персональных данных сторонним организациям возможна только в случаях, указанных федеральными законами и иными нормативными актами Российской Федерации, а также на условиях, определенных настоящим соглашением и законодательством.

Кроме того, передача персональных данных возможна без предварительного согласия субъекта в следующих ситуациях, предусмотренных частью 1 статьи 6 Федерального закона № 152-ФЗ «О персональных данных»:

Исполнение обязательств по договору, стороной которого является субъект персональных данных.

Необходимость исполнения судебных постановлений, предписаний государственных органов и иных властных структур.

Выполнение законных функций, назначенных управляющей компании органами исполнительной власти или суда.

Реализация общественных интересов, обеспечивающих защиту жизни, здоровья или иных жизненно важных интересов субъекта персональных данных.

Во всех остальных случаях, передача данных третьим лицам возможна не только с согласия субъекта, но и в ряде других обоснованных и законодательно разрешенных ситуаций, перечисленных в статье 6 закона № 152-ФЗ.

Процедура действий при утечке или неправомерного доступа к персональным данным, включая порядок информирования пользователей и соответствующие уполномоченные органы.

1. Выявление факта инцидента:
Оператором незамедлительно устанавливается факт произошедшего события, связанного с нарушением конфиденциальности персональных данных (утечка, хищение, несанкционированный доступ, модификация данных и т.д.). Факт происшествия фиксируется ответственным лицом управляющей компании.
2. Оценка последствий:
Определяются возможные последствия утраты или компрометации персональных данных, включая риск причинения вреда правам и интересам субъектов персональных данных.
3. Информирование руководства:
Ответственное лицо незамедлительно уведомляет руководство управляющей компании обо всех обстоятельствах случившегося и возможных последствиях.
4. Организация расследования:
Проводится внутреннее расследование обстоятельств происшествия силами собственной службы безопасности или привлеченных специалистов с целью установления причины инцидента, виновных лиц и степени ущерба.
5. Принятие оперативных мер:
Осуществляются немедленные технические и организационные мероприятия по предотвращению распространения угрозы и минимизации последствий утечки данных (блокировка учетных записей, изменение паролей, отключение уязвимых сервисов и устройств и т.д.).

6. Уведомление субъектов персональных данных:

Субъекты персональных данных оперативно информируются о факте утечки, её причинах и мерах, принимаемых управляющей компанией для устранения последствий. Информирование проводится путем направления письменного уведомления или электронного письма каждому затронутому лицу, если количество пострадавших превышает определённый порог (установленный внутренним порядком или законодательством).

7. Сообщение в государственные органы:

Управляющая компания обязана проинформировать Роскомнадзор и правоохранительные органы о произошедшем инциденте в течение установленного законом срока (не позднее 72 часов с момента обнаружения факта утечки). Предоставляется информация о характере инцидента, количестве пострадавших, принятых мерах и предложениях по устранению рисков повторения аналогичных ситуаций.

8. Проведение внутреннего аудита:

По результатам инцидента проводится внутренний аудит системы защиты персональных данных с целью выявления недостатков и разработки мероприятий по повышению уровня защиты.

9. Корректировка документации:

При необходимости вносятся изменения в политику обработки персональных данных и внутренние регламенты, направленные на устранение причин возникновения подобного инцидента.

Согласие субъекта на обработку персональных данных

В целях исполнения договора управления согласие на обработку персональных данных не требуется

Процедура рассмотрения запросов субъектов персональных данных

Субъекты персональных данных обладают правом на получение необходимой информации, внесение изменений или корректировок в личные данные, прекращение их обработки либо подачу жалоб контролирующим органам в случае нарушений.

Обращения принимаются в письменной форме через официальный канал связи управляющей компании. Рассмотрение поступивших запросов осуществляется в срок до 30 рабочих дней после поступления заявления.

Ответственность оператора

Нарушение настоящей Политики и правил обработки персональных данных влечет установленную законодательством Российской Федерации ответственность оператора, предусмотренную статьей 24 Федерального закона № 152-ФЗ «О персональных данных». В случае выявленного несоблюдения норм субъекты персональных данных вправе обращаться в судебные органы или компетентные инстанции.

Заключение

Политика вступает в силу немедленно и применяется бессрочно до внесения соответствующих изменений управляющим органом компании.

Измененная версия публикуется на официальном веб-сайте управляющей компании.

Контакты для подачи запросов:

- Сайт: <https://krg.brusnika.ru/>
- E-mail: tmn.dom@brusnika.ru
- Почта: 640002, г. Курган, ул. Коли Мяготина, д. 78, этаж 4, помещение 402
- Горячая линия: + 7 (3452) 38 28 78, +7 (3522) 42 88 88

Версия: 2025

Дата утверждения руководителем управляющей компании: 15 августа 2025 г.

Руководитель: /

