ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ KRASSKY

Цель настоящей Политики конфиденциальности – предоставить физическому лицу – клиенту общества с ограниченной ответственностью SIA Krassky (далее в тексте – Компания) – информацию о целях, объеме обработки персональных данных, их защите, сроке обработки и правах субъекта данных во время получения данных, а также при обработке персональных данных клиента.

АДМИНИСТРАТОР И ЕГО КОНТАКТНАЯ ИНФОРМАЦИЯ

Администратором данных, ответственным за обработку ваших данных, является SIA Krassky, рег. Номер 40003774722. Компания несет ответственность за безопасное хранение, обработку и удаление ваших данных. Если у вас возникнут вопросы об обработке персональных данных, свяжитесь, пожалуйста, с Компанией, отправив письмо на адрес эл. почты: krassky@krassky.lv, либо по телефону 67781400.

СФЕРА ПРИМЕНЕНИЯ ДОКУМЕНТА

Персональными данными является любая информация об идентифицированном или идентифицируемом физическом лице. Категории и примеры персональных данных указаны ниже:

Категория данных	Примеры
Данные клиента и делового партнера	Имя, фамилия, место работы и должность, персональный код, номер банковского счета, адрес, номер телефона, номер мобильного телефона, адрес эл. почты, адрес в Facebook, дата именин, дата рождения, предпочитаемый язык общения.
Данные кандидата на работу (физического лица, претендующего на вакансию в Компании)	Имя, фамилия, номер телефона, адрес эл. почты, адрес профиля на сайте LinkedIn, полученное резюме.

Политика конфиденциальности применяется для обеспечения конфиденциальности и защиты персональных данных в отношении перечисленных ниже субъектов данных (далее в тексте – Клиенты):

- физических лиц – клиентов и других пользователей услуг Компании (в том числе потенциальных, бывших и текущих), а также третьих лиц, которые в связи с оказанием услуг физическому лицу (клиенту, партнеру) получают или передают Компании какую-либо информацию (в том числе контактные лица, плательщики и др.);
- посетителей салонов, офисов, складов и других помещений Компании, в том числе тех, за которыми ведется видеонаблюдение;
- посетителей интернет-страниц Компании и лиц, которые звонят по телефонным номерам, зарегистрированным на имя Компании;
- физических лиц, претендующих на свободные вакансии в Компании.

Компания заботится о конфиденциальности и защите персональных данных Клиентов, соблюдает права Клиентов на законность обработки персональных данных согласно применимым правовым актам – Регламенту Европейского парламента и Совета от 27 апреля 2016 года № 2016/679 о защите физических лиц при обработке персональных данных и свободном обороте таких данных (далее в тексте – Регламент) и другим применимым правовым актам в области конфиденциальности и обработки данных.

Политика конфиденциальности распространяется на обработку данных независимо от того, в какой форме и/или среде Клиент предоставляет персональные данные (на домашней интернет-странице, в мобильных приложениях, на портале самообслуживания, в бумажном формате или по телефону) и в каких системах Компании или в бумажной форме осуществляется их обработка.

Для специфических видов обработки данных (например, обработки cookie-файлов и т. д.), а также для среды и целей обработки могут быть установлены дополнительные специфические положения, о которых Клиент уведомляется в момент предоставления Компании соответствующих данных.

ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания Krassky осуществляет обработку данных в следующих целях:

- оказание услуг и продажа товаров:
    - для идентификации Клиента;
    - для подготовки, заключения договора и доказательства факта заключения договора;
    - для доставки товаров и оказания услуг (исполнения договорных обязательств);
    - для обеспечения деятельности по оказанию услуг;
    - для исполнения гарантийных обязательств;
    - для улучшения товаров и услуг, разработки новых товаров и услуг;
    - для продвижения использования услуги, ее рекламы и распространения;
    - для обслуживания Клиентов;
    - для рассмотрения и обработки обращений и возражений;
    - для удержания Клиентов, укрепления лояльности, измерения уровня удовлетворенности;
    - для администрирования расчетов;
    - для возврата и взыскания долгов;
    - для содержания домашних страниц и мобильных приложений и улучшения их работы;
- бизнес-планирование и аналитика:
    - для статистики и бизнес-аналитики;
    - для планирования и учета;
    - для измерения эффективности;
    - для обеспечения качества данных;
    - для проведения исследований рынка и общественного мнения;
    - для подготовки отчетов;
    - для проведения опросов Клиентов;
    - в рамках мероприятий по управлению риском;
- обеспечение безопасности информации, информационных систем и Компании.
- Для предоставления информации органам государственного управления и субъектам оперативной деятельности в случаях и в объеме, установленных государственными и муниципальными нормативными актами;
- оценка соответствия кандидатов на вакантные должности.
- В других специфических целях, о которых Клиент уведомляется в момент предоставления Компании соответствующих данных.

ПРАВОВОЕ ОСНОВАНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания осуществляет обработку данных физического лица на следующих правовых основаниях:

- Согласие Клиента – Клиент, являясь субъектом персональных данных, сам дает согласие на сбор и обработку персональных данных в определенных целях. Согласие Клиента является его свободным волеизъявлением и самостоятельным решением, которое может быть дано в любой момент, что позволяет Компании осуществлять обработку персональных данных в определенных целях. Согласие Клиента является для него обязывающим, если дается в устной (во время телефонного разговора после идентификации Клиента) или письменной (при заполнении бланка в салоне Компании, при отправке электронного запроса после идентификации Клиента) форме. Клиент вправе в любое время отозвать свое ранее данное согласие, используя указанные каналы связи с Компанией. Отзыв согласия не оказывает влияния на законность обработки, основанной на согласии до отзыва.
- Согласие кандидата на работу – кандидат на вакантную должность в Компании, являясь субъектом персональных данных, сам дает согласие на сбор и обработку персональных данных в целях, позволяющих Компании максимально точно оценить соответствие кандидата вакантной должности. Согласие кандидата на работу является его свободным волеизъявлением и самостоятельным решением, которое может быть дано в любой момент, что позволяет Компании осуществлять обработку персональных данных в определенных целях. Согласие кандидата на работу является для него обязывающим, если дается в устной (во время телефонного разговора после идентификации кандидата) или письменной (при заполнении бланка в салоне Компании, при отправке электронного запроса) форме. Кандидат на работу вправе в любое время отозвать свое ранее данное согласие, используя указанные каналы связи с Компанией. Отзыв согласия не оказывает влияния на законность обработки, основанной на согласии до отзыва.
- Заключение и исполнение договора – для того чтобы Компания могла заключить и исполнить договор с Клиентом, качественно оказывая услуги и обслуживая Клиента, ей необходимо обобщить и обработать определенные персональные данные, собранные до заключения договора с Компанией или в период действия уже заключенного договора.
- Исполнение юридических обязательств – Компания вправе осуществлять обработку персональных данных в целях исполнения требований нормативных актов, а также для предоставления ответов на правомерные запросы государственных и муниципальных органов.
- Защита жизненно важных интересов – Компания вправе осуществлять обработку персональных данных в целях защиты жизненно важных интересов Клиента или иного

физического лица, например, если обработка необходима в гуманитарных целях, для мониторинга стихийных бедствий и антропогенных катастроф, в частности эпидемий и их распространения, или в исключительных гуманитарных ситуациях (террористические акты, техногенные катастрофы и т. д.).

- Исполнение официальных полномочий или общественные интересы – Компания вправе осуществлять обработку данных для выполнения задачи, осуществляемой в общественных интересах или при реализации официальных полномочий, законно предоставленных Компании.
  В таких случаях основания для обработки персональных данных изложены в нормативных актах.
- Легитимные (законные) интересы Компании или третьего лица – с учетом интересов Компании, основанных на предоставлении Клиенту качественных услуг и своевременной поддержки, Компания вправе осуществлять обработку данных физического лица в объеме, объективно необходимом и достаточном для достижения целей, указанных в настоящей Политике. Компания имеет следующие легитимные интересы:
  - вести коммерческую деятельность;
  - оказывать услуги Компании;
  - выполнять проверку личности Клиента перед заключением договора;
  - обеспечивать исполнение договорных обязательств;
  - устранять необоснованные финансовые риски для своей коммерческой деятельности (в том числе проводить оценку кредитного риска перед продажей товаров и услуг и во время исполнения договора);
  - осуществлять хранение заявок и обращений Клиентов на покупку товаров и оказание услуг, иных заявок и обращений, примечаний к ним, в том числе сделанных в письменной или устной форме по телефонам Компании и на домашних интернет-страницах;
  - осуществлять запись разговоров с Клиентом по вопросам деятельности, связанной с обеспечением услуг, ее поддержания, расчетов в целях контроля качества обслуживания клиентов;
  - осуществлять запись разговоров с Клиентом для организации исполнения договорных обязательств в рамках услуги;
  - осуществлять запись разговора с Клиентом, в ходе которого заключается устный договор, чтобы доказать факт заключения договора;
  - анализировать работу домашних страниц, интернет-страниц и мобильных приложений Компании, разрабатывать и внедрять улучшения к ним;
  - осуществлять действия по удержанию Клиентов;
  - сегментировать клиентскую базу данных для более эффективного предоставления услуг;
  - разрабатывать и продвигать товары и услуги;
  - рекламировать товары и услуги Компании;
  - отправлять другие сообщения о ходе исполнения договора и важных для исполнения договора событиях, а также проводить опросы Клиентов о товарах и услугах и опыте их использования;
  - предотвращать мошенничество;
  - обеспечивать корпоративное управление, бизнес-учет, учет финансов и аналитику;
  - обеспечивать эффективные процессы управления Компанией;
  - обеспечивать эффективность оказания услуг и продажи товаров, а также доставки;
  - обеспечивать и повышать качество услуг;
  - администрировать платежи;
  - администрировать невыполненные платежи;
  - отбирать лучшего кандидата на работу в Компании;
  - обращаться в органы государственного управления и оперативной деятельности, а также в суд для защиты своих правовых интересов;
  - информировать общество о деятельности Компании.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания осуществляет обработку данных Клиента, используя возможности современных технологий, с учетом существующих рисков конфиденциальности и разумно доступных для Компании организационных, финансовых и технических ресурсов.

Для обеспечения качественного и оперативного исполнения обязательств по заключенному с Клиентом договору Компания может уполномочить своих деловых партнеров осуществлять отдельные виды деятельности, связанные с поставкой товаров или оказанием услуг, например доставку товаров, выставление счетов и т. п. Если при выполнении данных задач деловые партнеры осуществляют обработку персональных данных Клиента, находящихся в распоряжении Krassky, соответствующие деловые партнеры считаются операторами обработки данных Krassky (обработчиками) и Компания вправе передавать деловым партнерам персональные данные Клиента, необходимые для осуществления указанных действий, в объеме, требуемом

для их осуществления.

Деловые партнеры Компании (в статусе обработчика персональных данных) будут обеспечивать исполнение требований по обработке и защите персональных данных в соответствии с требованиями Компании и положениями правовых актов, а также не будут использовать персональные данные в иных целях, а только для исполнения обязательств по договору/соглашению, заключенному с Клиентом, по поручению Krassky.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания защищает данные Клиента, используя возможности современных технологий, с учетом существующих рисков конфиденциальности и разумно доступных для Компании организационных, финансовых и технических ресурсов, в том числе принимая следующие меры безопасности:

- шифрование данных при их передаче (шифрование SSL);
- шифрование данных на серверах;
- межсетевые экраны;
- программы для защиты от взлома и выявления его попыток;
- другие защитные меры в соответствии с актуальными возможностями развития техники.

КАТЕГОРИИ ПОЛУЧАТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания не разглашает третьим лицам персональные данные Клиента или любую информацию, полученную в ходе оказания услуг и в период действия договора, в том числе информацию о полученных услугах, кроме следующих случаев:

- если соответствующему третьему лицу данные должны быть переданы в рамках заключенного договора для выполнения какой-либо функции, требуемой для исполнения договора или делегированной по закону (например, банку в рамках расчетов или для обеспечения услуги, например доставки товара, о чем уведомляется Клиент);
- в соответствии с четким и недвусмысленным согласием Клиента;
- лицам, предусмотренным внешними нормативными актами, по их обоснованному запросу в порядке и объеме, установленных внешними нормативными актами;
- в случаях, установленных внешними нормативными актами, для защиты легитимных интересов Krassky, например при обращении в суд или иные государственные учреждения против лица, нарушившего легитимные интересы Компании.

ПРОДОЛЖИТЕЛЬНОСТЬ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания осуществляет хранение и обработку персональных данных Клиента до тех пор, пока выполняется как минимум один из следующих критериев:

- только в течение срока действия заключенного с Клиентом договора (включая записи разговоров, в ходе которых заключается устный договор / подается заявка на услугу);
- данные необходимы для достижения цели, для которой они получены;
- до тех пор, пока в порядке, установленном внешними нормативными актами, Krassky или Клиент могут реализовывать свои легитимные интересы (например, предъявить возражения или подать в суд иск или вести иск в суде);
- до тех пор, пока у какой-либо из сторон имеется юридическая обязанность осуществлять хранение данных (например, согласно нормативным актам Латвийской Республики, компания должна хранить счета в течение 5 лет и др.);
- до тех пор, пока действует согласие Клиента на соответствующую обработку персональных данных при отсутствии другого законного основания для обработки данных.
- После прекращения действия обстоятельств, упомянутых в данном пункте, персональные данные Клиента удаляются. Контрольные журналы аудита хранятся не менее одного года со дня их составления в соответствии с положениями нормативных актов.

ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ И ДРУГИЕ ПРАВА КЛИЕНТА

Согласно положениям нормативных актов, Клиент вправе запросить у Krassky доступ к своим персональным данным, а также запросить у Компании их дополнение, исправление или удаление, или ограничение обработки в отношении Клиента, или право возразить против обработки (в том числе против обработки персональных данных, осуществляемой на основании легитимных интересов Компании), а также право на перенос данных. Данные права осуществляются в той мере, в какой обработка данных не вытекает из обязанностей компании Krassky, возложенных на нее действующими нормативными актами и осуществляемых в интересах общества.

Клиент может подать запрос об осуществлении своих прав:

- лично в письменной форме в салоне Компании по адресу: ул. Дунтес, 3, Рига, предъявив удостоверяющий личность документ;
- по электронной почте, отправив запрос на адрес: krassky@krassky.lv и подписав его надежной

электронной подписью.

После получения запроса Клиента об осуществлении своих прав Krassky удостоверяет личность Клиента, оценивает запрос и исполняет его в соответствии с положениями нормативных актов.

Компания отправляет Клиенту ответ по почте на указанный им контактный адрес заказным письмом или с учетом указанного Клиентом способа получения ответа.

Krassky обеспечивает исполнение требований по обработке и защите данных согласно положениям нормативных актов и в случае возражений Клиента предпринимает целесообразные действия для разрешения возражений. Однако, если достигнуть этого не удается,

Клиент вправе обратиться в надзорное учреждение – Государственную инспекцию данных.

СОГЛАСИЕ КЛИЕНТА НА ОБРАБОТКУ ДАННЫХ И ПРАВО ОТОЗВАТЬ СОГЛАСИЕ

Клиент может дать согласие на обработку персональных данных, правовым основанием которой является согласие, на интернет-страницах Компании (например, посредством формы подписки на рассылку новостей), по телефону или лично в одном из салонов Компании.

Клиент вправе в любой момент отозвать предоставленное согласие на обработку данных тем же способом, каким оно было дано, а именно: по телефону, путем отправки письма по электронной почте или лично в одном из салонов Krassky, и в таком случае дальнейшая обработка данных, основанная на ранее предоставленном согласии для конкретной цели, осуществляться не будет.

Отзыв согласия не влияет на обработку данных, осуществленную в период, когда согласие Клиента имело силу.

При отзыве согласия не может быть прекращена обработка данных, осуществляемая на основании других законных оснований.

СВЯЗЬ С КЛИЕНТОМ

Компания осуществляет связь с Клиентом, используя предоставленную Клиентом контактную информацию (номер телефона, адрес эл. почты, почтовый адрес).

Компания осуществляет связь по вопросам исполнения договорных обязательств в рамках услуги на основании заключенного договора (например, поставки товаров или услуг, информация о счетах, изменениях в услугах и др.).

КОММЕРЧЕСКИЕ УВЕДОМЛЕНИЯ

Связь, касающаяся коммерческих уведомлений об услугах Компании и/или третьих лиц, а также других уведомлений, не связанных с прямым обеспечением оговоренных услуг (например, опросы Клиентов), осуществляется Krassky с согласия Клиента или в соответствии с положениями внешних нормативных актов.

Клиент может дать согласие на получение коммерческих уведомлений от Компании и/или ее деловых партнеров на интернет-страницах Компании (например, посредством формы подписки на рассылку новостей), по телефону или лично в салонах Компании.

Предоставленное Клиентом согласие на получение коммерческих уведомлений действует до его отзыва (также после прекращения договора об оказании услуг). Клиент вправе в любое время отказаться от дальнейшего получения коммерческих уведомлений одним из следующих способов:

- отправив письмо на адрес эл. почты: krassky@krassky.lv;
- позвонив по телефону 67781400;
- лично в одном из салонов Компании;
- воспользовавшись предусмотренной в коммерческом уведомлении автоматизированной возможностью отказаться от дальнейшего получения уведомлений – нажав на указание об отказе, размещенное в заключительной части соответствующего коммерческого уведомления (электронного письма).

Компания прекращает отправку коммерческих уведомлений сразу после обработки запроса Клиента. Длительность обработки зависит от технологических возможностей и может составлять до семи суток.

Высказывая свое мнение в опросах и оставляя свою контактную информацию (адрес эл. почты, номер телефона), Клиент соглашается с тем, что компания Krassky может связаться с ним по поводу данной Клиентом оценки, воспользовавшись оставленной Клиентом контактной информацией.

ИСПОЛЬЗОВАНИЕ COOKIE-ФАЙЛОВ НА ИНТЕРНЕТ-СТРАНИЦАХ KRASSKY

На домашних страницах Компании используются cookie-файлы. Cookie-файлы – это небольшие текстовые

файлы, которые интернет-браузер (например, Chrome, Mozilla Firefox, Safari и др.) сохраняет на конечном устройстве пользователя (компьютере, мобильном телефоне, планшете) в момент посещения пользователем интернет-страницы в целях идентификации интернет-браузера либо сохранения в интернет-браузере информации или настроек. Таким образом cookie-файлы позволяют интернет-странице сохранять индивидуальные настройки пользователя, распознавать его и реагировать соответствующим образом, улучшая опыт пользования сайтом. Пользователь может отказаться от использования cookie-файлов или ограничить их использование, однако без cookie-файлов полноценное использование всех функций интернет-страниц будет невозможным.

В зависимости от выполняемых функций и цели использования Компания использует следующие cookie-файлы:

- Обязательные cookie-файлы
  Эти cookie-файлы необходимы для того, чтобы пользователь мог свободно посещать и просматривать интернет-страницу, пользуясь предлагаемыми возможностями, в том числе получать информацию о новостях и продуктах. Эти cookie-файлы идентифицируют устройство пользователя, однако не раскрывают его личность, а также не собирают и не обобщают информацию. Без этих cookie-файлов интернет-страница не сможет полноценно функционировать, например предоставлять пользователю необходимую информацию. Эти cookie-файлы хранятся на устройстве пользователя до закрытия интернет-браузера.
- Функциональные cookie-файлы
  С помощью функциональных cookie-файлов сайт запоминает выбранные пользователем настройки и сделанный выбор, что делает использование сайта более удобным. Эти cookie-файлы постоянно хранятся на устройстве пользователя.
- Аналитические cookie-файлы
  Аналитические cookie-файлы обобщают информацию о том, как пользователь использует интернет-страницу, выявляют наиболее посещаемые разделы, включая контент, выбираемый пользователем в процессе просмотра интернет-страницы. Информация используется в аналитических целях, чтобы выяснить, что интересует пользователей интернет-страницы, и впоследствии улучшить ее функциональность, сделав интернет-страницу более удобной в использовании. Аналитические cookie-файлы идентифицируют только устройство пользователя, но не раскрывают его личность. В отдельных случаях некоторые аналитические cookie-файлы вместо владельца сайта в соответствии с его указаниями и только в указанных целях управляются третьими лицами – обработчиками (операторами) данных, например Google Analytics.
- Таргетные (рекламные) cookie-файлы
  Таргетные (рекламные) cookie-файлы используются для обобщения информации о посещенных пользователем интернет-страницах и предложениях продуктов Компании или деловых партнеров, интересующих конкретного пользователя, либо для формирования предложений, соответствующих проявленному конкретным пользователем интересу. Как правило, эти cookie-файлы с разрешения владельца сайта в соответствии с указанными целями размещают третьи лица, например Google Ads. Таргетные cookie-файлы постоянно хранятся на конечном устройстве пользователя.

Krassky использует cookie-файлы в следующих целях:

- для улучшения пользовательского опыта посетителей сайтов и домашних страниц:
- для обеспечения функциональности домашней страницы;
- для адаптации функциональности домашней страницы к привычкам пользователя, включая язык, поисковые запросы, ранее просмотренный контент;
- для сбора статистических данных о потоке посетителей страницы – количестве посетителей, проведенном на странице времени, географической принадлежности, используемом устройстве и др.;
- для выдачи контента и предложений, создаваемых или распространяемых Компанией.

Продолжительность хранения cookie-файлов

Если не указано иное, cookie-файлы хранятся до тех пор, пока выполняется действие, для которого они собирались, и впоследствии удаляются.

Информация cookie-файлов не передается на обработку за пределы Европейского союза и стран ЕЭЗ.

Подтверждение и отключение cookie-файлов

При посещении сайтов и домашних страниц Компании пользователь видит окно с сообщением о том, что на интернет-странице используются cookie-файлы. Закрывая данное сообщение, пользователь подтверждает, что ознакомился с информацией о cookie-файлах, целях их использования, случаях передачи собранной ими информации третьему лицу, и выражает свое согласие с их использованием. Соответственно, правовым основанием для использования cookie-файлов является согласие пользователя. Настройки безопасности любого интернет-браузера позволяют ограничивать и удалять cookie-файлы. Однако необходимо учитывать, что отказаться от использования обязательных и функциональных cookie-файлов нельзя, поскольку без них полноценное использование сайта и домашних страницы невозможно.

На домашних страницах Krassky могут быть размещены ссылки на интернет-страницы третьих лиц, где действуют собственные условия использования и защиты персональных данных, ответственность за которые Компания не несет.

ПРОЧИЕ ПОЛОЖЕНИЯ

Компания вправе вносить изменения в Политику конфиденциальности, предоставляя Клиенту ее актуальную версию на домашней странице Компании www.krassky.lv.

KRASSKY ПРАВИЛА БЕЗОПАСНОСТИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

1. **Используемые термины:**
   Администратор – SIA Krassky, единый регистрационный номер 540003774722, юридический адрес: ул. Дунтес, 3, Рига, далее в тексте – Общество.
   Объект – Салон Krassky на 1-м и 6-м этажах в Риге, на улице Дунтес 3, офисные помещения на 2-м и 4-м этажах, в Риге, на улице Дунтес 3.
   Общий регламент о защите данных – Регламент Европейского парламента и Совета (ЕС) от 27 апреля 2016 года № 2016/679 о защите физических лиц при обработке персональных данных и свободном обороте таких данных, которым отменена директива № 95/46/ЕС (Общий регламент о защите данных).
   Система видеонаблюдения – осуществление видеозаписи камерами видеонаблюдения и просмотр в онлайн-системе, результатом чего является получение изображений и аудиозаписей идентифицируемых лиц или иной информации, относящейся к идентифицируемым физическим лицам.

   Ответственное лицо – работник SIA Krassky согласно распоряжению.

2. **Общие положения**
   2.1. Правила безопасности Системы видеонаблюдения Общества (далее в тексте – Правила) определяют порядок обработки персональных данных – изображения и звука – в Системе видеонаблюдения на Объекте, общие технические и организационные требования к ней в соответствии с требованиями нормативных актов, регламентирующих защиту данных физических лиц.
   2.2. Правила определяют:
      2.2.1. какими техническими ресурсами обеспечиваются обработка и безопасность персональных данных;
      2.2.2. какова продолжительность хранения записей видеонаблюдения;
      2.2.3. в каких случаях и в каком порядке разрешается доступ к видеонаблюдению в режиме онлайн и к архиву записей с камер видеонаблюдения;
      2.2.4. как соблюдаются требования безопасности видеонаблюдения в ежедневном режиме;
      2.2.5. лицо, ответственное за технические вопросы;
      2.2.6. размещение знаков, предупреждающих о ведении видеонаблюдения.
   2.3. Осуществляя видеонаблюдение, Общество:
      2.3.1. руководствуется единым пониманием и требованиями защиты в отношении видеонаблюдения как способа обработки данных физических лиц;
      2.3.2. избегает рисков и возможных нарушений, связанных с обработкой данных физических лиц, которые могут повлечь за собой неблагоприятные для Общества правовые и/или материальные последствия.
   2.4. Правила разработаны на основе положений Общего регламента о защите данных и иных нормативных актов, регулирующих защиту данных физических лиц, а также рекомендаций и руководств Государственной инспекции данных относительно обработки данных в сфере видеонаблюдения и защиты персональных данных на рабочем месте.
   2.5. Правила являются обязывающими для всех пользователей Системы видеонаблюдения: правления Общества, Ответственного лица, работников, осуществляющих просмотр и контроль изображения с камер видеонаблюдения в режиме реального времени, или иных лиц, которых Общество в определенных случаях наделяет соответствующим правом доступа к работе с Системой видеонаблюдения, – они обязуются также соблюдать требования, указанные в инструкции по использованию программного обеспечения оборудования.
   2.6. Оборудование Системы видеонаблюдения и видеокамеры устанавливаются таким образом, чтобы обеспечить соответствующее качество изображения и звука, с учетом технической спецификации, а также места или среды их размещения.
   2.7. Если в ходе видеонаблюдения не удается получить изображение, позволяющее идентифицировать субъект данных (изображение имеет низкое разрешение), требования настоящих Правил в области защиты данных физических лиц не применяются.
   2.8. Камеры видеонаблюдения не могут использоваться для записи разговоров между людьми. Оборудование не оснащено функцией аудиозаписи либо она должна быть отключена. Ответственное лицо обеспечивает отсутствие аудиозаписи во время видеонаблюдения.

3. Цель видеонаблюдения:

3.1. Цель видеонаблюдения – предупреждение и раскрытие преступных деяний, охрана жизни, здоровья и имущества лиц, а также соблюдение интересов других членов общества и обеспечение общественного порядка.

3.2. Общество, принимая во внимание то, что Объект является общественным местом, посещаемым широким кругом лиц, а также то, что на Объекте организуются мероприятия с повышенными требованиями к безопасности, выражает уверенность в том, что польза от осуществления видеонаблюдения превысит угрозу конфиденциальности физического лица и что оно обеспечит достижение цели, указанной в пункте 3.1 Правил, способом, наименее ущемляющим право лица на конфиденциальность.

3.3. При осуществлении видеонаблюдения соблюдается установленное внешними нормативными актами и Правилами регулирование видеонаблюдения как вида обработки данных.

4. Технические ресурсы, которыми обеспечиваются обработка и безопасность персональных данных:

4.1. Сбор персональных данных осуществляется с помощью непрерывно работающих камер видеонаблюдения.

4.2. Для обработки персональных данных на Объекте используются 26 (количество) камер, размещенных внутри помещений.

4.3. Технические ресурсы Общество использует в соответствии с требованиями, установленными производителем; их правильное использование обеспечивает безопасность и функционирование Системы видеонаблюдения.

4.4. Функционирование Системы обеспечивает устройство видеозаписи, информация хранится на жестком диске до 15 (пятнадцати) дней.

4.5. Просмотр изображения с камер видеонаблюдения на мониторе в режиме реального времени осуществляют администраторы в рабочие дни с 07:00 до 21:00, а с 21:00 до 07:00 и в выходные дни в 24-часовом режиме видеонаблюдение обеспечивается путем подключения к технической системе охранной сигнализации. Доступ к информации о записях имеют только Ответственное лицо и член правления Общества.

4.6. Доступ к техническим ресурсам имеет только Ответственное лицо. Ответственное лицо в случаях, определенных нормативными актами, может продемонстрировать записанную информацию другому лицу, указав информацию, упомянутую в пункте 6.5 настоящих Правил, при наличии предварительного разрешения члена правления Общества, в котором указана причина раскрытия таких данных.

4.7. Ответственное лицо, получив письменный запрос от правоохранительных органов о выдаче видеозаписи, подготавливает запись запрашиваемого фрагмента видеозаписи и указывает информацию, упомянутую в пункте 6.5 настоящих Правил.

4.8. Общество использует программное обеспечение в соответствии с требованиями, указанными в лицензии на соответствующее программное обеспечение.

4.9. В помещении, где осуществляется обработка персональных данных (место расположения сервера или компьютера):

4.9.1. температура не должна быть ниже +10 °C и выше +30 °C;

4.9.2. поддержка физических условий для оборудования носителей данных обеспечивается за счет отопления и вентиляции в помещении;

4.9.3. установлены переносные средства пожаротушения;

4.9.4. непрерывность работы технических ресурсов обеспечивается системой бесперебойного питания (UPS).

4.10. Резервное копирование системных записей не является обязательным. Решение о необходимости обеспечить резервные копии принимает лицо, ответственное за безопасность информационной системы.

4.11. У всех входов на Объект Ответственное лицо обеспечивает размещение информационного сообщения о ведении видеонаблюдения (приложение 1).

5. Место и продолжительность хранения записей видеонаблюдения:

5.1. Степень ценности информации оценивается как средневысокая.

5.2. По степени конфиденциальности информация считается информацией ограниченного доступа.

5.3. Данные записей видеонаблюдения классифицируются как информация ограниченного доступа, доступ к которой разрешен только Ответственному лицу.

5.4. Продолжительность хранения записей системы видеонаблюдения составляет до 15 (пятнадцати) суток. По истечении указанного срока записи автоматически удаляются в хронологическом порядке с момента выполнения записи.

5.5. Видеозаписи с камер видеонаблюдения, осуществляемого на Объекте, хранятся в устройстве видеозаписи, находящемся на Объекте. В случае проведения работ по обслуживанию или ремонту Системы видеонаблюдения Ответственное лицо обеспечивает перенос архива записей видеонаблюдения на внешний носитель информации.

6. Меры безопасности в отношении доступа к Системе видеонаблюдения

6.1. Для обеспечения безопасности данных в установленной Обществом Системе видеонаблюдения и видеозаписывающем оборудовании, а также для фиксации всех случаев просмотра и копирования данных должны соблюдаться следующие требования:

6.1.1. записи Системы видеонаблюдения выполняются в электронном виде и хранятся не дольше 15 (пятнадцати) суток с момента выполнения записи. Записи удаляются автоматически в хронологическом порядке с момента выполнения записи. При выявлении противоправных действий, для раскрытия которых необходимы видеозаписи, данные хранятся столько времени, сколько требуется;

6.1.2. Общество назначает Ответственное лицо для доступа к Системе видеонаблюдения и содержащимся в ней персональным данным (записям);

6.1.3. ручное удаление, копирование или передача персональных данных (записей), содержащихся на любого вида записывающем устройстве Системы видеонаблюдения, субъекту данных или правоохранительным органам осуществляется только по письменному запросу компетентного государственного органа. Удаление, копирование или передача записи третьим лицам осуществляется только с письменного разрешения члена правления Общества после указания информации, упомянутой в пункте 6.5 настоящих Правил.

6.2. Доступ к видеозаписям с камер видеонаблюдения ограничен и делится на два типа:

6.2.1. режим онлайн-просмотра;

6.2.2. режим просмотра архива.

6.3. Администраторы и Ответственное лицо имеют доступ ко всем установленным Обществом Системам видеонаблюдения в режиме онлайн-просмотра.

6.4. Доступ к режиму просмотра архива есть только у Ответственного лица и члена правления Общества. Права администратора Системы видеонаблюдения есть только у Ответственного лица.

6.5. Если необходимо передать данные, в соответствующих регистрационных листах фиксируются следующие случаи:

6.5.1. просмотр данных (записей) на устройстве видеозаписи (приложение 2);

6.5.2. копирование данных (записей) с устройства видеозаписи на другие носители данных (приложение 3);

6.5.3. передача данных (записей) с устройства видеозаписи субъекту данных, третьим лицам и правоохранительным органам (приложение 2);

6.5.4. удаление видеозаписи (приложение 4).

6.6. Определенные учреждения вправе запрашивать и получать имеющиеся в распоряжении Общества записи с камер видеонаблюдения согласно положениям внешних нормативных актов для исполнения своих обязанностей, установленных нормативными актами.

6.7. Субъект данных вправе запросить записи с камер видеонаблюдения, но только те, которые относятся к этому субъекту данных. Если на видеозаписи видно и идентифицируется другое физическое лицо, Общество должно обеспечить неразглашение его данных (изображения), например, сделав это изображение неотображаемым. Если продолжительность видеозаписи составляет несколько часов, а субъект данных виден на ней только в течение нескольких минут, субъекту выдается только эта часть записи.

7. Чрезвычайные обстоятельства:

7.1. При возникновении чрезвычайных ситуаций защита работы Системы видеонаблюдения обеспечивается в соответствии с правилами пожарной безопасности в помещениях. Технические ресурсы, на которых хранятся персональные данные, следует по возможности перенести в безопасное место.

7.2. Общество обеспечивает документацию в достаточном объеме, чтобы иметь возможность вносить изменения в Систему или полностью восстановить ее в случае возникновения угрозы.

7.3. При возникновении чрезвычайной ситуации для восстановления работы Системы видеонаблюдения используются аналогичные технические ресурсы.

8. Средства защиты технических ресурсов от преднамеренного повреждения и несанкционированного завладения:

8.1. Общество обеспечивает охрану помещений. Помещения оснащены технической охраной с подключением к пульту круглосуточного наблюдения, включая систему пожарной сигнализации, тревожные кнопки, а также пост физической охраны (круглосуточно).

8.2. Технические ресурсы Системы хранятся в помещениях, закрываемых после окончания рабочего

времени.

8.3. Помещения, в которых осуществляется обработка персональных данных (где находится сервер или компьютер, на котором хранится запись), не доступны посторонним лицам.

8.4. Пароль доступа к персональным данным (записям) известен только Ответственному лицу.

8.5. Логическая безопасность обработки персональных данных обеспечивается установленной системой управления контентом, которая предотвращает исправление или удаление персональных данных без санкционированного доступа. Доступ к редактированию данных имеется только у конкретного субъекта персональных данных.

9. Право субъекта данных на получение данных видеонаблюдения:

9.1. Субъект данных имеет право доступа к информации о видеонаблюдении, имеющейся в распоряжении Администратора (в том числе если она технически доступна), однако ее невозможно исправить или дополнить, поскольку в противном случае это будет считаться фальсификацией или искажением информации.

9.2. Ответственное лицо обеспечивает резервирование копии видеоматериала путем извлечения видеоматериала из локального видеоархива:

9.2.1. при получении запроса – Общество регистрирует его и передает на исполнение Ответственному лицу. Правоохранительный орган выдает подтверждение о получении запрошенной информации, заверив его именем, фамилией, должностью конкретного лица и датой на информации носителя данных. Запрос с вышеуказанным заверением хранится в номенклатурном деле Общества;

9.2.2. при получении жалобы от лица, в том числе анонимной, которую Ответственное лицо в контексте целей видеонаблюдения оценивает как достаточную для обработки запроса на резервирование данных (например, если субъект не идентифицирован в очном порядке, но получено анонимное сообщение о том, что замечено, как работник неправомерно принял некое благо);

9.2.3. если произошло событие, автоматически информирующее о признаках инцидента в сфере безопасности, или если Ответственное лицо подало запрос на резервирование данных в соответствии с требованиями внутреннего контроля;

9.2.4. если от субъекта данных получено письменное заявление, содержащее информацию для идентификации запрошенных данных, и субъект данных идентифицирован в очном порядке согласно требованиям пункта 9.5.

9.3. Ответственное лицо выдает субъекту данных фотофиксацию (-и) из видеоматериала, не раскрывая данные фотофиксации других лиц, а также описание видеоматериала и/или разъяснение аудиозаписи, не раскрывая данные аудиозаписи других лиц. Субъекту данных выдается фотофиксация, наиболее точно соответствующая основанию для запроса данных видеонаблюдения.

9.4. Если субъект данных не идентифицирован до получения запроса на резервирование данных, данные видеонаблюдения выдаются субъекту данных только в том случае, если субъект данных подал письменное заявление и субъект данных идентифицирован в очном порядке.

9.5. Для получения данных видеонаблюдения субъект данных является к Ответственному лицу на Объект или в Общество по его юридическому адресу:

9.5.1. субъект данных предъявляет Ответственному лицу или работнику Общества документ, удостоверяющий личность, подает письменное заявление, указав в нем:

9.5.1.1. основание для запроса данных видеонаблюдения;

9.5.1.2. дату, время и место (в том числе местонахождение видеокамеры, если оно известно), где снят видеоматериал;

9.5.1.3. описание ситуации или события (в котором зафиксированы данные видеонаблюдения субъекта данных);

9.5.1.4. подробное описание внешнего вида субъекта данных, содержащее информацию об одежде и вещах, которые были при себе у субъекта данных, и конкретного места нахождения субъекта данных, где он находился;

9.5.1.5. иную информацию, которая существенна для идентификации запрошенных данных;

9.5.1.6. желаемый срок получения данных видеонаблюдения;

9.5.1.7. при невозможности незамедлительной выдачи данных видеонаблюдения подается одна цветная фотография, на которой субъект данных изображен в полный рост и по которой субъект данных может быть визуально идентифицирован в соответствии с фотографией в документе, удостоверяющем личность.

9.6. Субъект данных вправе получить только данные видеонаблюдения, где виден или слышен конкретный субъект данных, чей внешний вид совпадает с поданной фотографией и описанием внешнего вида. Данные видеонаблюдения не выдаются при отсутствии достаточной уверенности в обоснованности запроса данных видеонаблюдения и сходстве субъекта данных в видеоматериале.

9.7. Субъект данных не имеет права получать данные видеонаблюдения, на которых видны или слышны другие субъекты данных. По этой причине субъекту данных выдается информация о видеонаблюдении только в установленном виде, но не выдаются копии видеоматериала в отредактированном виде, в частности, потому что в соответствии с объемом, контекстом и целями видеонаблюдения, осуществляемого Ответственным лицом и Обществом:

9.7.1. в месте видеонаблюдения могут находиться другие субъекты данных, данные которых не подлежат раскрытию (ни в идентифицированном, ни в неидентифицированном виде);

9.7.2. подготовленный в отредактированном виде видеоматериал может создать ложное представление об истинном ходе событий.

9.8. Информация о видеонаблюдении субъекту данных не выдается, если запрос субъекта данных очевидно не обоснован (в том числе не связан с целями видеонаблюдения или отсутствуют достаточные основания для запроса данных видеонаблюдения) либо требует чрезмерных усилий, в частности из-за регулярного повторения.

9.9. На каждое письменное обращение субъекта данных, в том числе в связи с реализацией своих прав, Общество предоставляет ответ в течение одного месяца, за исключением установленных в нормативных актах субъектов данных, ответ которым предоставляется в более короткий срок.

9.10. Если реализация прав субъекта данных заключается в получении информации о видеонаблюдении, Ответственное лицо по возможности учитывает указанный субъектом данных желаемый срок получения данных видеонаблюдения. Если ответ невозможно предоставить в течение одного месяца или иного срока, установленного нормативным актом, субъекту данных предоставляется промежуточный ответ и сообщается о сроке предоставления информации.

9.11. Если субъект данных считает, что в зоне видеонаблюдения произошло нарушение прав субъекта данных и необходимо срочно представить доказательства, субъект данных вправе обратиться в правоохранительные органы. Соответственно в таком случае Общество подготавливает и предоставляет информацию в ответ на такой запрос на резервирование данных.

9.12. Общество сотрудничает с правоохранительными органами в рамках запросов на любую информацию при наличии угрозы безопасности для отдельных лиц или общественности, а также в рамках процесса обмена данными, чтобы обеспечить правоохранительным органам доступ к необходимой информации.

10. Порядок расследования инцидентов в сфере безопасности

10.1. Инцидентом в сфере безопасности считается повреждение оборудования Системы или несанкционированная попытка доступа к информации, а также утрата информации или части оборудования.

10.2. При выявлении нарушения защиты персональных данных либо инцидента в сфере безопасности Системы, а также нарушений настоящих Правил или их последствий Ответственное лицо предпринимает следующие действия: 10.2.1. проверяет ручные и электронные контрольные журналы аудита и их целостность на предмет доступа к Системе и приостанавливает работу Системы до тех пор, пока не будут выяснены риски и причины инцидента;

10.2.2. запрашивает письменное пояснение у лица, причастного к нарушению защиты персональных данных или инциденту в сфере безопасности;

10.2.3. вносит в реестр нарушений (приложение 5) запись о произошедшем нарушении защиты персональных данных или наличии возможного инцидента в сфере безопасности;

10.2.4. выясняет причины нарушения защиты персональных данных или инцидента в сфере безопасности и при необходимости разрабатывает поправки к Правилам, вводящие дополнительные требования к защите;

10.2.5. принимает решение о влиянии риска на права субъекта данных;

10.2.6. если нарушение защиты персональных данных или инцидент в сфере безопасности может привести к риску для прав и свобод субъекта данных, Ответственное лицо ставит в известность Общество, которое незамедлительно сообщает о нарушении защиты данных в Государственную инспекцию данных и CERT.lv, но не позднее чем через 72 часа с момента, когда стало известно об инциденте в сфере безопасности;

10.2.7. если установлено, что нарушение защиты персональных данных или инцидент в сфере безопасности может представлять высокий риск для прав и свобод субъекта данных, Общество незамедлительно сообщает об этом субъекту данных;

10.2.8. в случае необходимости виновный работник привлекается к ответственности.

10.3. При возникновении подозрений о совершении преступного деяния (кража персональных данных) Общество незамедлительно сообщает об этом в правоохранительные органы.

10.4. В случае инцидентов в сфере безопасности Системы проводится проверка и при необходимости

внедряются иные меры безопасности.

10.5. Форма уведомления об инциденте в сфере безопасности при обработке персональных данных, адресуемого Государственной инспекции данных, размещена по адресу: http://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas- parkapuma-pazinojuma-iesniegsana/.

11. Заключительные положения:

Предусмотренные Правилами требования безопасности пересматриваются один раз в год, а также в случае внесения изменений в нормативные акты.

Приложение 1
к Правилам безопасности системы видеонаблюдения

ВЕДЕТСЯ ВИДЕОНАБЛЮДЕНИЕ

Цель: предупреждение и раскрытие преступных деяний, охрана жизни, здоровья и имущества лиц, а также соблюдение интересов других членов общества и обеспечение общественного порядка по адресу: ул. Дунтес, 4 (4-й этаж), Рига.

Администратор: SIA Krassky, единый регистрационный номер 540003774722, юридический адрес: ул. Дунтес, 3, Рига.

Подробная информация о правах субъекта данных размещена на домашней странице Администратора krassky.lv либо ее можно получить, отправив запрос на адрес эл. почты: krassky@krassky

Приложение 2

к Правилам безопасности системы видеонаблюдения

Лист регистрации просмотра/передачи третьим лицам видеозаписей (персональных данных), выполненных системой видеонаблюдения на объекте недвижимости по адресу ул. Дунтес, 3, Рига, № 1

№ п/п	Дата и время	Имя, фамилия, должность третьего лица, участвовавшего в просмотре данных	Подпись третьего лица или адрес отправки	Подпись ответственного лица	Причина просмотра/ передачи записи	Дата и время, за какой период выполнен просмотр/передача записи
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Приложение 3

к Правилам безопасности системы видеонаблюдения

Лист регистрации копирования на другие носители данных видеозаписей (персональных данных), выполненных системой видеонаблюдения на объекте недвижимости по адресу ул. Дунтес, 3, Рига, № 2

№ п/п	Дата и время	Имя, фамилия, должность лица, участвовавшего в копировании данных	Подпись ответственного лица	Причина копирования записи	Дата и время, за какой период выполнено копирование записи
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Приложение 4
к Правилам безопасности системы видеонаблюдения

Лист регистрации удаления видеозаписей (персональных данных), выполненных системой видеонаблюдения на объекте недвижимости по адресу ул. Дунтес, 3, Рига, № 3

№ п/п	Дата и время	Имя, фамилия, должность лица, участвовавшего в удалении данных	Подпись ответственного лица	Причина удаления записи	Дата и время, за какой период выполнено удаление записи
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Приложение 5
к Правилам безопасности системы видеонаблюдения

Реестр нарушений (инцидентов)

№	Администратор	Вовлеченный обработчик	Инцидент (характеристика)	Дата	Влияние	Управление	Значимость инцидента