ПОЛИТИКА (ПОЛОЖЕНИЕ)
Общества с ограниченной ответственностью «УК А» в отношении обработки и защиты персональных данных

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» (далее – Закон о ПДн) и является основополагающим внутренним регулятивным документом общества с ограниченной ответственностью «УК БРИГ» (далее – Управляющая организация), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Управляющая организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Управляющей организации, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Управляющей организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Если в отношениях с Управляющей организацией участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Управляющая организация становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Управляющей организации распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Управляющей организацией.

2. Основания обработки и состав персональных данных, обрабатываемых в Управляющей организации

2.1. Обработка ПДн в Управляющей организации осуществляется в связи с выполнением законодательно возложенных на Управляющую организацию функций, определяемых:

1) Жилищным Кодексом РФ;

2) Постановлением Правительства РФ № 354 от 06.05.2011 г. «О предоставлении коммунальных услуг собственникам и пользователям помещений в многоквартирных домах и жилых домов»;

3) Постановлением Правительства РФ от 13.08.2006 №491 «Об утверждении Правил содержания общего имущества в многоквартирном доме и правил изменения размера платы за содержание и ремонт жилого помещения в случае оказания услуг и выполнения работ по управлению, содержанию и ремонту общего имущества в многоквартирном доме ненадлежащего качества и (или) с перерывами, превышающими установленную продолжительность»;

4) Постановлением Правительства РФ № 416 от 15.05.2013 г. « О порядке осуществления деятельности по управлению многоквартирными домами».

2.2. В рамках осуществления функции по управлению многоквартирным домом, ПДн обрабатываются Управляющей организацией:

1) в ходе предоставления потребителям коммунальных услуг;

2) начисления платы за коммунальные услуги и подготовки платежных документов потребителям;

3) при проведении проверки правильности исчисления предъявленного потребителю к уплате размера платы за коммунальные услуги, задолженности или переплаты потребителя за коммунальные услуги, правильности исчисления потребителю пени.

4) подготовки претензий при выявлении нарушения потребителем действующего законодательства РФ;

5) подготовки документов в судебные инстанции при наличии задолженности по жилищно-коммунальным услугам, нарушения режима использования общего имущества многоквартирного

дома;

6) при проведении проверки достоверности переданных потребителем сведений о показаниях приборов учета;

При этом обрабатываются ПДн:

а) потребителей, пользующихся на праве собственности или ином законном основании помещениями в многоквартирном доме, потребляющих коммунальные услуги.

2.3. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Управляющая организация выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство в Управляющую организацию, работников Управляющей организации (далее - Работники) и бывших Работников.

2.4. В связи с реализацией своих прав и обязанностей, Управляющей организацией обрабатываются ПДн физических лиц, являющихся контрагентами Управляющей организации по гражданско-правовым договорам, физических лиц, ПДн которых используются для осуществления пропускного режима в Многоквартирный дом, а также граждан, письменно обращающихся в Управляющую организацию по вопросам его деятельности (помимо лиц, указанных в пунктах 2.2 Политики).

2.5. Специальные категории персональных данных, а также биометрические персональные данные Управляющей организацией не обрабатываются.

2.6. ПДн получаются и обрабатываются Управляющей организацией на основании федеральных законов.

2.7. В целях исполнения возложенных на Управляющую организацию функций Управляющая организация в установленном порядке вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым Управляющая организация поручает обработку ПДн, включаются условия, обязывающие таких лиц соблюдать предусмотренные Законом о ПДн и Политикой правила обработки ПДн.

2.8. Управляющая организация предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

2.9. В Управляющей организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Управляющей организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Управляющей ПНд передаются во вновь избранную Управляющую организацию в соответствии с ч.10 ст.162 ЖК РФ.

2.10. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Управляющая организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Управляющей организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Управляющая организация руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Управляющей организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Управляющей организации (далее - ИС) и других имеющихся в Управляющей организации систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Управляющей организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Управляющей организации (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Управляющей организации (далее - СЗПДн) не дают возможности преодоления имеющихся в Управляющей организации систем защиты возможными нарушителями безопасности ПДн;

11) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

12) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

13) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Управляющей организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Управляющей организации до заключения договоров;

14) наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

15) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в Управляющей организации ПДн имеют лица, уполномоченные приказом Управляющей организации, а также лица, чьи ПДн подлежат обработке.

4.2. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Управляющей организации. Допуск Работников к обработке ПДн осуществляется согласно перечню полномочий, утверждаемых в должностной инструкции. Допущенные к обработке ПДн Работники под роспись знакомятся с документами Управляющей организации, устанавливающими порядок обработки ПНд, включая документы, устанавливающие права и обязанности конкретных Работников.

4.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Управляющей организацией, осуществляется в соответствии с Законом о персональных данных и определяется внутренними регулятивными документами Управляющей организации.

5. Реализация Политики

5.1. Управляющая организация принимает необходимые и достаточные меры для защиты

обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки ПДн в Управляющей организации несет Управляющий объектом, а также лица, определяемые приказом Генерального директора Управляющей организации.

Ответственный за организацию обработки ПДн в Управляющей организации, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением в Управляющей организации требований нормативных правовых актов и внутренних регулятивных документов Управляющей организации в области обработки и защиты ПДн;

2) доводить до сведения Работников положения нормативных правовых актов и внутренних регулятивных документов Управляющей организации в области обработки и защиты ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. Управляющая организация осуществляет обработку ПДн без использования средств автоматизации, а также с использованием таких средств.

5.4. При обработке ПДн без использования средств автоматизации Управляющая организация, в соответствии с положениями нормативных правовых актов в области обработки и защиты ПДн, реализует комплекс организационных и технических мер, обеспечивающих:

1) обособление ПДн от информации, не содержащей ПДн;

2) раздельную обработку и хранение каждой категории ПДн (фиксация на отдельных материальных носителях ПДн, цели обработки которых заведомо несовместимы);

3) соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, установленным требованиям;

4) соблюдение установленных требований при ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в помещения, занимаемые Управляющей организацией, или в иных аналогичных целях;

5) сохранность материальных носителей ПДн;

6) условия хранения, исключающие несанкционированный доступ к ПДн, а также смешение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

7) надлежащее уточнение, уничтожение или обезличивание ПДн.

5.5. В соответствии с требованиями нормативных правовых актов в области обработки и защиты ПДн обработки ПДн с использованием средств автоматизации в Управляющей организации создаются ИСПДн.

Все ИСПДн проходят периодическую классификацию и аттестацию в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности ПДн.

5.6. Обработка ПДн в Управляющей организации с использованием средств автоматизации ведется только в ИСПДн. В Управляющей организации запрещается обработка ПДн с целями, не соответствующими целям создания ИСПДн, эксплуатация ИСПДн в составе, отличном от указанного при создании ИСПДн.

5.7. В целях обеспечения управления информационной безопасностью ПДн в Управляющей организации создается СЗПДн.

Объектами защиты СЗПДн являются информация, обрабатываемая Управляющей организацией и содержащая ПДн.

5.8. СЗПДн реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

1) подготовку внутренних регулятивных документов Управляющей организации по вопросам обработки и защиты ПДн, контроль за исполнением в Управляющей организации требований нормативных правовых актов и внутренних регулятивных документов Управляющей организации в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы;

2) оформление письменных обязательств Работников о неразглашении ПДн;

3) доведение до сведения Работников информации об установленных законодательством

Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

4) обеспечение наличия в должностных обязанностях Работников требований по соблюдению установленного порядка обработки и защиты ПДн;

5) разработку и введение в действие внутренних регулятивных документов Управляющей организации по обеспечению информационной безопасности ИСПДн;

6) регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

7) ознакомление Работников с положениями нормативных правовых актов и внутренних регулятивных документов Управляющей организации в области обработки и защиты ПДн, а также обучение Работников правилам обработки и защиты ПДн;

8) регламентацию обработки ПДн, в том числе хранения и передачи информации как внутри Управляющей организации, так и при взаимодействии с контрагентами Управляющей организации, государственными органами и организациями, обращения с документами (включая электронные документы) и носителями, порядка их учета, хранения и уничтожения;

9) установление правил доступа на объекты, в помещения, в ИС, применению в этих целях систем охраны и управления доступом;

10) организацию технического оснащения объектов и ИСПДн в соответствии с существующими требованиями к информационной безопасности;

11) формирование условий и технологических процессов обработки, хранения и передачи информации в Управляющей организации (включая условия хранения документов в архивах), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и внутренних регулятивных документов Управляющей организации в области обработки и защиты ПДн;

12) установление полномочий пользователей и форм представления информации пользователям ИСПДн;

13) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

14) организацию необходимых мероприятий с Работниками, а также собеседование с лицами, претендующими на работу в Управляющей организации, изучение их биографии и проверку предоставляемых сведений; обучение Работников требованиям информационной безопасности;

15) осуществление контроля эффективности организационных мер защиты;

16) разработку защитных технических решений:

а) выборе технических средств обработки информации;

б) разработке и (или) приобретении программного обеспечения;

5.9. Для всех критичных в отношении обеспечения целостности и доступности ПДн функций ИСПДн разрабатываются соответствующие планы обеспечения непрерывной работы и восстановления при авариях и стихийных бедствиях, которые не реже одного раза в квартал проходят актуализацию. Работники проходят обучение необходимым действиям по обеспечению целостности и доступности ПДн в нештатных ситуациях.

6. Основные мероприятия по обеспечению безопасности персональных данных

6.1. Мероприятия по защите ПДн реализуются в Управляющей организации в следующих направлениях:

1) предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;

2) предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

3) защита от вредоносных программ;

4) обеспечение безопасного межсетевого взаимодействия;

5) обеспечение безопасного доступа к сетям международного информационного обмена;

6) анализ защищенности ИСПДн;

7) обнаружение вторжений и компьютерных атак;

8) осуществления контроля за реализацией системы защиты ПДн.

6.2. Мероприятия по обеспечению безопасности ПДн включают в себя:

1) реализацию разрешительной системы допуска пользователей (Работников) к информационным ресурсам ИС и связанным с их использованием работам, документам;

2) разграничение доступа пользователей ИСПДн и обслуживающих ИСПДн Работников к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

3) регистрацию действий пользователей и обслуживающих ИСПДн Работников, контроль несанкционированного доступа и действий пользователей и обслуживающих Работников, а также третьих лиц;

4) использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

5) предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов;

6) ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

7) размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

8) организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

9) учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

10) резервирование технических средств, дублирование массивов и носителей информации;

11) реализацию требований по безопасному межсетевому взаимодействию ИС;

12) использование защищенных каналов связи, защита информации при ее передаче по каналам связи;

13) межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИС;

14) обнаружение вторжений в ИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

15) периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на ИС;

16) активный аудит безопасности ИС на предмет обнаружения в режиме реального времени несанкционированной сетевой активности.

6.4. С целью поддержания состояния защиты ПДн на надлежащем уровне в Управляющей организации осуществляется внутренний контроль за эффективностью системы защиты ПДн и соответствием порядка и условий обработки и защиты ПДн установленным требованиям.

Внутренний контроль включает:

1) мониторинг состояния технических и программных средств, входящих в состав СЗПДн;

2) контроль соблюдения требований по обеспечению безопасности ПДн (требований нормативных правовых актов и внутренних регулятивных документов в области обработки и защиты ПДн, требований договоров).

6.5. В целях осуществления внутреннего контроля в Управляющей организации проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в Управляющей организации либо комиссией, образуемой Генеральным директором Управляющей организации.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывается Генеральному директору Управляющей организации.