ключевые системы
и компоненты

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Содержание:

1. Введение

1.1. Назначение документа

Документ «Политика обработки и защиты персональных данных» (далее – Политика) ООО «КСК» (далее – Общество) определяет позицию и намерения Общества в области обработки и реализации требований к защите персональных данных лиц, состоящих в договорных, гражданско-правовых и иных отношениях с Обществом, соблюдения действующего законодательства Российской Федерации в области информационной безопасности, а также требований Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных», основной целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Политика предназначена для изучения и неукоснительного исполнения всеми работниками Общества, а также подлежит доведению до сведения лиц, состоящих в договорных, гражданско-правовых и иных отношениях с Обществом (далее – граждане), Контрагенты, Партнеры и другие заинтересованные стороны.

1.2. Область применения

Требования настоящей Политики распространяются на все подразделения Общества.

1.3. Нормативные ссылки

Перечень Внешних и Внутренних нормативных документов:

Внешние:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
- Трудовой кодекс РФ. Глава 14. «Защита персональных данных работника».
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
- Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Внутренние:

- Стандарт «Корпоративная Политика информационной безопасности» утв. приказом № КСК-0037/ОД от 12.04.2019.
- Стандарт «Положение о порядке обработки и обеспечения безопасности защищаемой информации» утв. приказом №КСК-0073/ОД от 17.07.2019.
- Стандарт «Положение об организации антивирусной защиты» утв. приказом №КСК-0075/ОД от 24.07.2019.

- Стандарт «Положение о допуске к информационным ресурсам ООО «КСК» утв. приказом №КСК-0111/ОД от 25.09.2019.
- «Перечень защищаемой информации, обрабатываемой в ООО «КСК» утв. приказом ОРД №КСК-0114/ОД от 30.09.2019.
- Стандарт «Тестирование программных, программно-аппаратных средств в ООО «КСК» утв. приказом №КСК-0120/ОД от 16.10.2019.
- СТО 7.1.3-05-2019 СМБ. Конфигурирование сетевого оборудования ООО «КСК» утв. приказом №КСК-0136/ОД от 30.10.2019.
- Стандарт «Обработка инцидентов информационной безопасности» утв. приказом №КСК-0135/ОД от 30.10.2019.
- СТО 7.1.3-06-2019 «Инструкция администратора по обеспечению безопасной обработки защищаемой информации» утв. приказом №КСК-0134/ОД от 30.10.2019.
- Стандарт «Обеспечение непрерывности работы, резервного копирования и восстановления данных».
- Стандарт «Эксплуатация СКЗИ в ООО «КСК».
- Стандарт «Инструкция ответственного за обеспечение защиты персональных данных».
- Стандарт «Инструкция ответственного за организацию обработки персональных данных».
- Стандарт «Инструкция пользователя по обеспечению безопасной обработки защищаемой информации».
- Стандарт «Модель угроз и нарушителя безопасности защищаемой информации ООО «КСК».
- Стандарт «Контроль защищенности, выявления и устранения уязвимостей в информационных системах ООО «КСК» утв. приказом №КСК-0143/ОД от 06.11.2019.
- Стандарт «Конфигурирование программных, программно-аппаратных средств в ООО «КСК» утв. приказом №КСК-0142/ОД от 06.11.2019.
- Стандарт «Реагирование на обращения субъектов персональных данных в ООО «КСК».

1.4. Термины, определения и сокращения

В настоящем Документе используются следующие термины и определения.

Департамент ИТ — Департамент информационных технологий Общества.

Обработка ПДн — любое действие (операция) или совокупность действий (операций) с ПДн, совершаемых с использованием средств автоматизации или без использования таких средств. К таким действиям (операциям) можно отнести: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Общество — Общество с ограниченной ответственностью «Ключевые Системы и Компоненты» (ООО «КСК»).

Отдел информационной безопасности (Отдел ИБ) — подразделение ответственное за информационную безопасность Общества.

Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Работник — физическое лицо, вступившее в трудовые отношения с работодателем в лице Общества.

РФ — Российская Федерация.

ФЗ — Федеральный закон.

2. Ответственность

2.1. Ответственность за организацию процесса обработки персональных данных в Обществе возлагается на Дирекцию по управлению персоналом.

2.2. Ответственность за организацию технических мероприятий по созданию системы защиты персональных данных в Обществе возлагается на Отдел ИБ и Департамент ИТ.

2.3. Лица, ответственные за организацию обработки и защиты персональных данных, получают указания непосредственно от Генерального директора Общества и подотчетны ему.

2.4. Общество несет ответственность за неисполнение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – ФЗ № 152-ФЗ) в соответствии с действующим законодательством Российской Федерации.

Конкретные наказания за определенные действия/бездействие в области обработки персональных данных содержат нормы Кодекса Российской Федерации об административных правонарушениях и Уголовного кодекса Российской Федерации.

3. Общие положения

3.1. Общество обеспечивает надежную защиту предоставленных ПДн. Общество обрабатывает ПДн только тех лиц, которые состоят в договорных, гражданско-правовых и иных отношениях с Обществом, а именно:

- лиц, состоящих в трудовых отношениях с Обществом (работники Общества);
- лиц, являющихся соискателями должностей в Обществе;
- лиц, являющихся Контрагентами или Партнерами Общества.

3.2. Под безопасностью ПДн Общество понимает защищенность ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн и принимает необходимые правовые, организационные и технические меры для защиты ПДн.

3.3. Обработка ПДн работников Общества осуществляется в строгом соответствии с трудовым законодательством РФ. Данные Контрагентов или Партнеров Общества, полученные в связи с заключением договора, стороной которого является субъект ПДн, обрабатываются с соблюдением принципов и условий обработки ПДн, установленных ФЗ № 152-ФЗ. Общество не осуществляет распространение или раскрытие ПДн без согласия гражданина, если иное не предусмотрено федеральным законом.

3.4. Правовым основанием обработки ПДн является осуществление возложенных на Общество законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, Федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» № 27-ФЗ от 01.04.1996 г., «О персональных данных» № 152-ФЗ от 27.07.2006 г., «Об обществах с ограниченной ответственностью» № 14-ФЗ от 08.02.1998 г., «Об электронной подписи» № 63-ФЗ от 06.04.2011 г., а также в целях организации учета служащих Общества для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия служащему в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования».

3.5. При обработке ПДн Общество придерживается следующих принципов:

- Общество осуществляет обработку ПДн только на законной и справедливой основе;
- обработка ПДн в Обществе ограничивается достижением конкретных, заранее определенных и законных целей;
- в Обществе не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

- до начала сбора/получения ПДн, Общество определяет конкретные законные цели обработки ПДн;
- Общество собирает только те ПДн, которые являются необходимыми и достаточными для заявленной цели обработки;
- Общество систематически принимает меры по удалению или уточнению неполных или неточных данных;
- Общество уничтожает либо обезличивает ПДн по достижении целей обработки или в случае утраты необходимости в достижении целей[1];
- Общество не раскрывает третьим лицам и не распространяет персональные данные без согласия гражданина (если иное не предусмотрено действующим законодательством Российской Федерации);
- Общество не осуществляет сбор и обработку персональных данных граждан, касающихся расовой, национальной принадлежности, политических, религиозных, философских и иных убеждений, состояния здоровья, интимной жизни, членства в общественных объединениях, в том числе в профессиональных союзах.

3.6. Общество вправе поручить обработку персональных данных (с согласия гражданина[2]) юридическому лицу, на основании заключаемого с этим лицом договора, в котором указанные лица обязуются соблюдать принципы и правила обработки персональных данных, предусмотренные ФЗ № 152-ФЗ. В договоре (поручении Общества) должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность ПДн при их обработке.

3.7. В случае осуществления Обществом трансграничной передачи ПДн граждан на территорию иностранного государства, указанная трансграничная передача должна осуществляться с соблюдением требований действующего законодательства Российской Федерации, а также международно-правовых актов. При этом получающей стороной могут быть страны, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, а также иные иностранные государства при условии обеспечения адекватных защитных мер прав субъектов ПДн.

4. Права граждан в части обработки персональных данных

4.1. Гражданин, ПДн которого обрабатываются в Обществе имеет право:

- требовать от Общества уточнения его ПДн их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отозвать свое согласие на обработку ПДн;
- требовать устранения неправомерных действий Общества в отношении его ПДн;
- обжаловать действия или бездействие Общества в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если гражданин считает, что Общество осуществляет обработку его ПДн с нарушением требований ФЗ № 152-ФЗ или иным образом нарушает его права и свободы;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

---

[1] Если иное не предусмотрено соглашением между Обществом и гражданином либо если Общество не вправе осуществлять обработку ПДн без согласия гражданина на основаниях, предусмотренных Законом «О персональных данных» или другими федеральными законами.

[2] Если иное не предусмотрено федеральным законом.

4.2. Гражданин имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Обществом;
- правовые основания и цели обработки ПДн;
- сведения о применяемых Обществом способах обработки ПДн;
- наименование и место нахождения Общества;
- сведения о лицах (за исключением работников Общества), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Обществом или на основании федерального закона;
- перечень обрабатываемых ПДн, относящихся к гражданину, от которого поступил запрос и источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления гражданином прав, предусмотренных Законом «О персональных данных»;
- информацию об осуществляемой или о предполагаемой трансграничной передаче ПДн;
- иные сведения, предусмотренные Законом «О персональных данных» или другими федеральными законами.

5. Сведения о реализуемых требованиях к защите персональных данных

Общество при обработке ПДн принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. К таким мерам, в соответствии с ФЗ № 152-ФЗ, относятся:

- назначение лица, ответственного за организацию обработки ПДн, и лиц, ответственных за обеспечение безопасности ПДн;
- определение угроз безопасности ПДн при их обработке;
- разработка и утверждение локальных актов по вопросам обработки и защиты ПДн;
- оценка вреда, который может быть причинен гражданам в случае нарушения ФЗ № 152-ФЗ, соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152-ФЗ;
- ознакомление работников Общества, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами по вопросам обработки и защиты ПДн, и обучение работников Общества;
- соблюдение условий, исключающих несанкционированный доступ к материальным носителям ПДн и к средствам защиты ПДн;
- применение технических мер защиты, включая:
  - средства разграничения доступа на сетевом, прикладном и общесистемном уровнях;
  - средства межсетевого экранирования;
  - средства регистрации и учета действий пользователей на сетевом, прикладном и общесистемном уровнях;
  - антивирусные средства защиты;
  - средства криптографической защиты информации;
  - средства обнаружения вторжений;
  - средства анализа защищенности;

- средства контроля физического доступа в помещения, в которых осуществляется обработка ПДн.
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию новой информационной системы Общества;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в информационных системах Общества, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн;
- осуществление внутреннего контроля и аудита соответствия обработки ПДн ФЗ № 152-ФЗ.

6. Внесение изменений

6.1. Политика утверждается и вводится в действие приказом Генерального директора Общества.

6.2. Настоящая Политика пересматривается не реже, чем раз в год.

6.3. Настоящая Политика подлежит изменению по мере необходимости:

- при изменении законодательства Российской Федерации в области ПДн;
- в случаях выявления несоответствий, затрагивающих обработку ПДн;
- по результатам контроля выполнения требований по обработке и защите ПДн;
- по решению руководства Общества.

6.4. Исключительным правом внесения изменений и дополнений в Политику, а также разработки ее новой редакции обладает Отдел ИБ.

6.5. Актуальная версия настоящей Политики публикуется на официальном сайте Общества – http://www.kscgroup.ru.

7. Справочная информация

7.1. Если после прочтения настоящей Политики у Вас остались вопросы, Вы можете получить разъяснения по всем интересующим вопросам, позвонив по телефону +7 (495) 788-19-50, либо направив официальный запрос по почте на адрес: Российская Федерация, 127055, г. Москва, ул. Бутырский Вал, д. 26, стр. 1. ООО «КСК».

7.2. В случае направления официального запроса в Общество, в тексте запроса необходимо указать:

- номер основного документа, удостоверяющего личность гражданина (или его законного представителя), сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие гражданина в отношениях с Обществом (например, номер и дата заключения договора) либо сведения, иным способом подтверждающие факт обработки ПДн Обществом;
- подпись гражданина (или его законного представителя). Если официальный запрос отправляется в электронном виде, то он должен быть оформлен в виде электронного документа и подписан электронной подписью в соответствии с законодательством РФ.