Документ введен в действие

Приказом № 47 от 17.01.2022 г.

УТВЕРЖДАЮ
Генеральный директор
Акционерного общества
«Сталепромышленная компания»

_____ А. Ю. Сухнев
(подпись)
« 07 » декабря 2021 г.

ПОЛИТИКА

в отношении обработки и защиты персональных данных в АО «Сталепромышленная компания»

2021 г.

Содержание

1. Назначение

1.1. Настоящая Политика Акционерного общества «Сталепромышленная компания» (далее – АО «СПК») в отношении обработки персональных данных (далее - Политика) разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее – 152-ФЗ) в целях обеспечения 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.

1.2. Политика действует в отношении всех персональных данных, которые обрабатывает АО «СПК» .

1.3. Политика распространяется на отношения в области обработки персональных данных, возникшие у АО «СПК» (Оператора) как до, так и после утверждения настоящей Политики.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Оператора.

1.5. Настоящая Политика опубликована на сайте АО «СПК» и к ней обеспечен неограниченный доступ.

2. Определения

2.1. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

2.2. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

2.3. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.4. **Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.5. **Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.6. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.7. **Оператор (Оператор персональных данных)** – государственный орган, муниципальный орган, юридическое или физическое лицо (АО «СПК») , самостоятельно или совместно с другими лицами организующие и (или)

осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

2.9. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.10. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.11. **Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

2.12. **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

3. Перечень условных обозначений и сокращений

ИСПДн — информационные системы персональных данных

ПДн — персональные данные

СЗПДн — система защиты персональных данных, обрабатываемых в информационных системах персональных данных

СЗИ — средство защиты информации

4. Права и обязанности Оператора

4.1. Оператор имеет право:

- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о ПДн или другими федеральными законами;

- поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку ПДн по поручению Оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные 152-ФЗ;

- в случае отзыва субъектом ПДн согласия на обработку ПДн Оператор вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в 152-ФЗ.

4.2. Оператор обязан:

- организовывать обработку ПДн в соответствии с требованиями 152-ФЗ;

- отвечать на обращения и запросы субъектов ПДн и их законных представителей в соответствии с требованиями 152-ФЗ;

- сообщать в уполномоченный орган по защите прав субъектов ПДн (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций - Роскомнадзор) по запросу этого органа необходимую информацию в течение 10 дней с даты получения такого запроса.

4.3. Основные права субъекта ПДн. Субъект ПДн имеет право:

- получать информацию, касающуюся обработки его ПДн, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту ПДн Оператором в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, когда имеются законные основания для раскрытия таких ПДн. Перечень информации и порядок ее получения установлен 152-ФЗ;

- требовать от Оператора 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, а также принимать предусмотренные законом меры по защите своих прав;

- выдвигать условие предварительного согласия при обработке ПДн в целях продвижения на рынке товаров, работ и услуг;

- обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его ПДн.

4.4. Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, ответственным за организацию обработки ПДн у Оператора.

4.5. Ответственность за нарушение требований законодательства Российской Федерации и нормативных актов АО «СПК» в сфере обработки и защиты ПДн определяется в соответствии с законодательством Российской Федерации.

5. Построение системы защиты персональных данных

5.1. Обработка ПДн, в АО «Сталепромышленная компания» (далее АО «СПК»), осуществляется в соответствии с требованиями Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных».

5.2. Защита ПДн, обрабатываемых без использования средств автоматизации, строиться на основании требований Постановления Правительства РФ от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5.3. Система защиты ПДн, обрабатываемых в информационных системах персональных данных АО «СПК» (далее СЗПДн), строиться на основании требований нормативных правовых актов, принятых в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», а также:

- Актов определения уровня защищенности ПДн при их обработке в ИСПДн АО «СПК»;

- Моделей угроз безопасности ПДн при их обработке в ИСПДн.

5.4. Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется в соответствии с порядком, установленным Постановлением Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5.5. СЗПДн включает в себя следующие подсистемы:

- Подсистема идентификации и аутентификации субъектов доступа и объектов доступа;

- Подсистема управления доступом субъектов доступа к объектам доступа;

- Подсистема защиты машинных носителей ПДн;

- Подсистема регистрации событий безопасности;

- Подсистема антивирусной защиты;

- Подсистема контроля (анализа) защищенности ПДн;

- Подсистема защиты среды виртуализации;

- Подсистема защиты технических средств;

- Подсистема защиты ИСПДн, ее средств, систем связи и передачи данных.

5.6. Состав требований, реализуемых каждой из подсистем СЗПДн, зависит от:

- Уровня защищенности ПДн при их обработке в ИСПДн;

- Структурно-функциональных характеристик и особенностей функционирования ИСПДн;

- Состава актуальных угроз безопасности ПДн при их обработке в ИСПДн.

6. Цели обработки персональных данных.

6.1. Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. В АО «СПК» не допускается обработка ПДн, несовместимых с целями сбора ПДн.

6.2. Обработка Оператором ПДн осуществляется в следующих целях:

- обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;

- фактически осуществляемой Оператором деятельности, а также деятельности, которая предусмотрена учредительными документами Оператора, и конкретных бизнес-процессов Оператора в конкретных ИСПДн (по структурным подразделениям Оператора и их процедурам в отношении определенных категорий субъектов ПДн);

- ведения кадрового делопроизводства;

- содействия работникам в трудоустройстве;

- получения образования и продвижении по службе;

- обеспечения личной безопасности работников;

- контроля количества и качества выполняемой работы;

- обеспечение сохранности имущества;

- привлечения и отбор кандидатов на работу у Оператора;

- организации постановки на индивидуальный (персонифицированный) учет работников в системе обязательного пенсионного страхования;

- заполнения и передачи в органы исполнительной власти и иные уполномоченные организации требуемых форм отчетности;

- осуществления гражданско-правовых отношений;

- ведения бухгалтерского учета;

- осуществления пропускного режима.

6.3. Обработка ПДн работников осуществляет исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

7. Правовые основания обработки персональных данных.

7.1. Правовым основанием обработки ПДн является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку ПДн, в том числе:

- Конституция Российской Федерации;

- Гражданский кодекс Российской Федерации;

- Трудовой кодекс Российской Федерации;

- Налоговый кодекс Российской Федерации;

- федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора (в т.ч., но не ограничиваясь:);

- уставные документы Оператора;

- договоры, заключаемые между Оператором и субъектом ПДн;

- согласие на обработку ПДн (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям Оператора).

8. Объемы и категории обрабатываемых персональных данных.

8.1. Содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Оператор не допускает избыточной обработки ПДн по отношению к заявленным целям их обработки.

8.2. Оператор может производить обработку следующих ПДн:

8.2.1. Кандидаты для приема на работу к Оператору:

- фамилия, имя, отчество;

- пол;

- гражданство;

- дата и место рождения;

- контактные данные;

- сведения об образовании, опыте работы, квалификации;

- иные ПДн, сообщаемые кандидатами в резюме и сопроводительных письмах.

8.2.2. Работники и бывшие работники Оператора:

- фамилия, имя, отчество;

- пол;

- гражданство;

- дата и место рождения;

- изображение (фотография) (небиометрическая);

- паспортные данные;

- адрес регистрации по месту жительства;

- адрес фактического проживания;

- контактные данные;

- индивидуальный номер налогоплательщика;

- страховой номер индивидуального лицевого счета (СНИЛС);

- сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;

- семейное положение, наличие детей, родственные связи;

- сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий;

- данные о регистрации брака;

- сведения о воинском учете;

- сведения об инвалидности;

- сведения об удержании алиментов;

- сведения о доходе с предыдущего места работы;

- иные ПДн, предоставляемые работниками в соответствии с требованиями действующего законодательства.

8.2.3. Члены семьи работников Оператора:

- фамилия, имя, отчество;

- степень родства;

- год рождения;

- иные ПДн, предоставляемые работниками в соответствии с требованиями действующего законодательства.

8.2.4. Клиенты и контрагенты Оператора (физические лица):

- фамилия, имя, отчество;

- дата и место рождения;

- паспортные данные;

- адрес регистрации по месту жительства;

- контактные данные;

- индивидуальный номер налогоплательщика;

- номер расчетного счета;

- иные ПДн, предоставляемые клиентами и контрагентами (физическими лицами), необходимые для заключения и исполнения договоров и в соответствии с требованиями действующего законодательства.

8.2.5. Представители (работники) клиентов и контрагентов Оператора (юридических лиц):

- фамилия, имя, отчество;

- паспортные данные;

- контактные данные;

- замещаемая должность;

- иные ПДн, предоставляемые представителями (работниками) клиентов и контрагентов, необходимые для заключения и исполнения договоров в соответствии с требованиями действующего законодательства.

8.3. Специальные категорий ПДн и биометрические персональные данные Оператором не обрабатываются.

9. Порядок и условия обработки персональных данных.

9.1. Обработка ПДн осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

9.2. Обработка ПДн осуществляется с согласия субъектов ПДн на обработку их ПДн, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

9.3. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку ПДн.

9.4. Оператор вправе передавать ПДн органам дознания и следствия, Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

9.5. Оператор не допускает раскрытие третьим лицам и распространение ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом 152-ФЗ. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, оформляется отдельно от иных согласий субъекта ПДн на обработку его ПДн.

9.6. К обработке ПДн допускаются работники Оператора, в должностные обязанности которых входит обработка ПДн.

9.7. Обработка ПДн осуществляется путем:

- получения ПДн в устной и письменной форме непосредственно от субъектов персональных данных;

- получения ПДн из общедоступных источников;

- внесения ПДн в журналы, реестры и информационные системы Оператора;

- использования иных законных способов обработки ПДн.

9.8. Оператор принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

- определяет угрозы безопасности ПДн при их обработке;

- принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты ПДн;

- назначает лиц, ответственных за обеспечение безопасности ПДн в структурных подразделениях и информационных системах Оператора;

- создает необходимые условия для работы с ПДн;

- организует учет документов, содержащих ПДн;

- организует работу с информационными системами, в которых обрабатываются ПДн;

- хранит ПДн в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

- организует обучение работников Оператора, осуществляющих обработку ПДн.

9.9. Оператор осуществляет хранение ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором.

9.10. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан (в т.ч. Российской Федерации) с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в 152-ФЗ.

10. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов персональных данных

10.1. Подтверждение факта обработки ПДн Оператором, правовые основания и цели обработки ПДн, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных 152-ФЗ, предоставляются Оператором субъекту ПДн или его представителю при обращении либо при получении запроса субъекта ПДн или его представителя.

В предоставляемые сведения не включаются ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, когда имеются законные основания для раскрытия таких ПДн.

Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта ПДн в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Оператором;

- подпись субъекта ПДн или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Если в обращении (запросе) субъекта ПДн не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных 152-ФЗ, в том числе если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

10.2. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование ПДн, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

В случае подтверждения факта неточности ПДн Оператор на основании сведений, представленных субъектом ПДн или его представителем либо Роскомнадзором, или иных необходимых документов уточняет ПДн в течение семи рабочих дней со дня представления таких сведений и снимает блокирование ПДн.

10.3. В случае выявления неправомерной обработки ПДн при обращении (запросе) субъекта ПДн или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, с момента такого обращения или получения запроса.

10.4. При достижении целей обработки ПДн, а также в случае отзыва субъектом ПДн согласия на их обработку ПДн подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

- Оператор не вправе осуществлять обработку без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом "О персональных данных" или иными федеральными законами;

- иное не предусмотрено иным соглашением между Оператором и субъектом ПДн.

11. Контроль за соблюдением законодательства и локальных нормативных актов АО «СПК» в области персональных данных, в том числе требований к защите персональных данных

11.1. Выделяются следующие группы лиц, участвующих в обработке и защите ПДн:

- ответственный за организацию обработки ПДн;

- администратор информационной безопасности;

- администратор;

- пользователи ИСПДн.

11.2. Ответственный за организацию обработки ПДн

11.2.1. Ответственный за организацию обработки ПДн – работник АО «СПК», обеспечивает:

- подготовку локальных актов АО «СПК» по вопросам обработки и защиты ПДн;

- осуществление внутреннего контроля за соблюдением АО «СПК» и его работниками законодательства Российской Федерации, локальных актов по вопросам обработки и защиты ПДн;

- проведение инструктажа работников в целях доведения до данных работников положений законодательства Российской Федерации, локальных актов по вопросам обработки и защиты ПДн;

- организацию приема и обработки запросов (обращений, заявлений) субъектов ПДн или их представителей.

11.2.2. Ответственный за организацию обработки ПДн несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией ответственного за организацию обработки ПДн» или соответствующим договором со специализированной организацией.

11.3.Администратор информационной безопасности

11.3.1. Администратор информационной безопасности – работник АО «СПК», ответственный за установку, настройку и сопровождение СЗИ.

11.3.2. Администратор информационной безопасности несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Положением об администраторе информационной безопасности».

11.4.Администратор

11.4.1. Администратор – работник АО «СПК», ответственный за установку, настройку и сопровождение программных, программно-аппаратных, аппаратных средств ИСПДн.

11.5. Пользователь ИСПДн

11.5.1. Пользователь ИСПДн – работник АО «СПК», осуществляющий обработку ПДн в ИСПДн.

11.5.2. Пользователь ИСПДн несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией пользователя ИСПДн».