

Политика общества с ограниченной ответственностью «Альфа-стом8» В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Гражданским Кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-методическими документами ФСТЭК России в сфере обработки персональных данных.

1.2. В настоящей Политике используются следующие понятия, термины и сокращения:

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

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, 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.

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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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.

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

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

Уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

1.3. Настоящая Политика и изменения к ней утверждаются Руководителем Общества с ограниченной ответственностью «Альфа-стом8» (далее — Общество).

1.4. Настоящая Политика вступает в силу с момента её утверждения и действует бессрочно, до замены её новой Политикой.

1.5. Настоящая Политика определяет организацию защиты персональных данных в Общества и является обязательной для исполнения всеми сотрудниками Общества, непосредственно осуществляющими обработку персональных данных и (или) имеющими доступ к персональным данным.

1.6. Целью Политики является определение правильного способа обработки персональных данных, а также разработка на его основе процедур, предотвращающих или реагирующих на нарушение безопасности персональных данных.

2. Обработка персональных данных

2.1. Принципы обработки персональных данных

2.1.1. В Обществе обрабатываются персональные данные следующих групп субъектов:

- работников, общества;
- граждан, включенных в кадровый резерв, граждан, но не прошедших конкурсный отбор;
- граждан, а также юридических лиц, обращающихся в Общество

2.1.2. Персональные данные относятся к категории конфиденциальной информации.

2.1.3. Обработка персональных данных в Обществе осуществляется на законной и справедливой основе.

2.1.4. Обработка персональных данных в Обществе ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.1.5. В Обществе не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.1.6. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.1.7. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки.

2.1.8. При обработке персональных данных в Обществе обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Общество принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

2.1.9. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.1.10. Сотрудники Общества, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.2. Условия обработки персональных данных

2.2.1 Обработка персональных данных в Обществе осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных».

Обработка персональных данных в Обществе допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для достижения уставных целей общества, в соответствующим законодательством Российской Федерации

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2.2.2 Общество вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение Общества). Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Общества определяются перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, устанавливается обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указываются требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

2.2.3 Лицо, осуществляющее обработку персональных данных по поручению Общества, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

2.2.4 В случае если Общество поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Общество. Лицо, осуществляющее обработку персональных данных по поручению Общества, несет ответственность перед Обществом.

2.3. Описание обработки персональных данных

2.3.1 Для осуществления обработки персональных данных субъектов персональных данных берется их согласие в соответствии с Федеральным законом «О персональных данных», за исключением случаев, предусмотренных федеральным законом.

2.3.2 При принятии решений, затрагивающих интересы субъекта, сотрудники Общества не имеют права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки.

2.3.3 Трансграничная передача персональных данных в Обществе не осуществляется.

2.3.4. Общество не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

2.3.5 Обработка персональных данных о судимости может осуществляться в соответствии с федеральными законами.

2.3.6 Общество осуществляет обработку (передачу) персональных данных субъектов ПДн с использованием бумажных, цифровых носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа на основании согласия субъекта ПДн, за исключением случаев, предусмотренных ст.6 Федерального закона «О персональных данных».

2.3.7 При передаче персональных данных субъекта сотрудники Общества соблюдают следующие требования:

- не сообщают персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных законодательством.
- предупреждают лица, получающие персональные данные субъектов, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требуют от этих лиц обеспечения конфиденциальности полученных персональных данных;
- не сообщают персональные данные субъекта в коммерческих целях без его письменного согласия;
- передают персональные данные субъекта представителям субъектов в порядке, установленном законодательством, и ограничивают эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;
- не отвечают на вопросы, связанные с передачей персональных данных субъекта по телефону или факсу.

2.3.8 В случае достижения цели обработки персональных данных Общество прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации.

2.3.9. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Общество прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации.

2.3.10 В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Общество осуществляет блокирование таких персональных данных или

обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

2.3.11 Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

3. Права субъекта персональных данных

3.1. Каждый субъект персональных данных имеет право:

- получать полную информацию о своих персональных данных и иметь свободный бесплатный доступ к своим персональным данным, получать копии любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных Федеральным законом «О персональных данных»;
- получать информацию, касающейся обработки его персональных данных, в том числе содержащей: подтверждение факта обработки, правовые основания и цель обработки; способы обработки, наименование и место нахождения Общества, сведения о лицах (за исключением сотрудников Общества), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании Федерального закона «О персональных данных»; обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом «О персональных данных»; сроки обработки персональных данных, в том числе сроки их хранения; порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»; наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу; иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами;
- требовать от сотрудников Общества, осуществляющих обработку персональных данных, уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- заявить о своем несогласии при отказе сотрудников Общества исключить или исправить персональные данные (в письменной форме с соответствующим обоснованием такого несогласия).

3. 2. Общество обязано безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к этому субъекту, а также внести в них необходимые изменения при предоставлении субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, в соответствующем законодательством РФ. О внесенных изменениях и предпринятых мерах Общества обязана уведомить субъекта или его представителя и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Защита персональных данных

4.1. Общество при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.2. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, используемых в процессе деятельности Общества

4.3. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер по устранению негативных последствий и проведением служебного расследования;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4.4. В целях организации контроля обеспечения безопасности персональных данных в Обществе создана постоянно действующая Комиссия по обеспечению безопасности персональных данных.

4.5. В Обществе приняты следующие правовые и организационные меры по защите персональных данных:

- назначен ответственный за организацию обработки персональных данных;
- назначен администратор безопасности ИСПДн для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн;
- определен перечень ИСПДн и состав ПДн, обрабатываемых в ИСПДн, в том числе на бумажных носителях;
- определен и утвержден перечень лиц, непосредственно осуществляющих обработку персональных данных в информационных системах персональных данных Общества и лиц, имеющих доступ к ПДн, обрабатываемым на бумажных носителях;
- определен и утвержден перечень лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе персональных данных;
- определен перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- определен перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- определены цели обработки персональных данных, сроки обработки и хранения ПДн;
- определены режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- ведется учет машинных носителей персональных данных;
- определены границы контролируемых зон;
- определены конфигурация и топология ИСПДн в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения;
- разработаны организационно-распорядительные документы, регламентирующие процесс обработки и защиты персональных данных;
- определены угрозы безопасности ПДн в конкретных условиях функционирования ИСПДн, разработаны Модели угроз безопасности ПДн при их обработке в ИСПДн;
- сотрудники Общества, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, локальными актами Общества по вопросам обработки персональных данных.

4.6. В Обществе осуществляется периодический внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Общества в отношении обработки персональных данных, локальным актам Общества.