

УТВЕРЖДЕНО

Приказом Президента Акционерного общества «Санкт-Петербургская Международная Товарно-сырьевая Биржа»

от «05» октября 2017 г. № 475

ПОЛИТИКА

**Акционерного общества «Санкт-Петербургская
Международная Товарно-сырьевая Биржа» в отношении
обработки персональных данных**

Москва 2017

Содержание

1. Общие положения	3
1.1.Термины, определения и сокращения	3
1.2.Правовые основания обработки персональных данных.....	4
1.3.Права и обязанности оператора и субъектов персональных данных.....	5
2. Цели обработки персональных данных субъектов персональных данных Общества.....	8
3. Категории обрабатываемых персональных данных, категории субъектов персональных данных.....	9
3.1.Категории обрабатываемых персональных данных.....	9
3.2.Категории субъектов персональных данных.....	9
4. Порядок и условия обработки персональных данных	10
5. Защита персональных данных в Обществе, обеспечение безопасной обработки персональных данных.....	12
6. Ответственность.....	13

1. Общие положения

1.1. Термины, определения и сокращения

Для целей настоящего документа используются следующие основные термины и сокращения:

Акционерное общество «Санкт-Петербургская Международная Товарно-сырьевая Биржа» - Общество, АО «СПбМТСБ»;

ИС – информационные системы;

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

конфиденциальность персональных данных - обязательное для соблюдения Обществом или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

ПО – программное обеспечение;

персональные данные - 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;

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;

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

субъект персональных данных — физическое лицо, которое может быть однозначно идентифицировано по персональным данным

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» — ФЗ «О персональных данных».

Термины, специально не определенные в настоящей Политике, используются в значениях, установленных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», нормативными актами Банка России, иными нормативными правовыми актами Российской Федерации, а также политикой Общества в отношении обработки персональных данных в порядке, определенном Законом, и иными внутренними документами Общества.

1.2. Правовые основания обработки персональных данных

Настоящая Политика Акционерного общества «Санкт-Петербургская Международная Товарно-сырьевая Биржа» (далее – Политика) в отношении обработки персональных данных определяет политику Общества, а также порядок организации и обеспечения безопасной обработки персональных данных субъектов персональных данных Общества.

Политика разработана в соответствии с законодательством Российской Федерации в области персональных данных с целью конкретизации мер по защите законных интересов субъектов персональных данных, определения правовых, организационных и технических решений по защите персональных данных, порядка обеспечения конфиденциальности персональных данных и обеспечения безопасности при их обработке.

Политика определяет требования к сбору, систематизации, накоплению, хранению, уточнению (обновлению, изменению), использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению персональных данных физических лиц, для которых Общество выступает в качестве оператора персональных данных (работники Общества, клиенты и другие субъекты персональных данных).

Требования, изложенные в настоящей Политике, являются обязательными для выполнения всеми лицами Общества, допущенными к обработке персональных данных, при этом срочность и важность выполняемых ими работ не должны являться основанием для нарушения требований Политики и других документов, регламентирующих в Обществе вопросы обработки и защиты персональных данных.

Пересмотр и обновление настоящей Политики осуществляется в связи с изменениями законодательства Российской Федерации в области персональных данных, по результатам анализа актуальности, эффективности и достаточности используемых мер обеспечения защиты персональных данных, а также по результатам других контрольных мероприятий.

Текущая редакция Политики вступает в силу с даты утверждения и размещается на сайте Общества в открытом доступе.

Перечень нормативных документов:

- Трудовой кодекс Российской Федерации;
- Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Получение и обработка персональных данных работников и клиентов в ИСПДн (ИС) Общества осуществляется с учетом принципов, установленных статьей 5 ФЗ «О персональных данных» исключительно в целях обеспечения соблюдения требований законодательства Российской Федерации и нормативных актов исполнительных органов государственной власти.

1.3.Права и обязанности оператора и субъектов персональных данных

1.3.1 Права и обязанности оператора

Согласно ФЗ «О персональных данных», Общество, как оператор персональных данных, имеет право:

- поручать обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено ФЗ «О персональных данных», на основании заключаемого с этим лицом договора;
- требовать от лица, которому поручена обработка персональных данных субъектов персональных данных Общества, соблюдения их конфиденциальности, на основании заключенных с ним договоров или соглашений о конфиденциальности данной информации;
- продолжать обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в статьях ФЗ «О персональных данных» в случае отзыва субъектом персональных данных согласия на обработку персональных данных;
- осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных в случаях, указанных в статьях ФЗ «О персональных данных».

Общество, как оператор персональных данных, имеет иные права, установленные ФЗ «О персональных данных».

Обязанности оператора персональных данных:

В случаях установленных законодательством Российской Федерации в области персональных данных, Общество обязано:

- сообщать в порядке, предусмотренном статьей 14 ФЗ «О персональных данных», субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить безвозмездно возможность ознакомления с этими персональными данными;
- сообщать в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию;
- осуществлять блокирование неправомерно обрабатываемых персональных данных, при обращении (по запросу) субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных или обеспечивать их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае подтверждения факта неточности персональных данных уточнить персональные данные либо обеспечить их уточнение;
- уничтожать персональные данные или обеспечить их уничтожение в случае, если обеспечить правомерность обработки персональных данных невозможно, об устранении допущенных нарушений или об уничтожении персональных данных уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган;
- прекращать обработку персональных данных или обеспечивать ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожать персональные данные или обеспечивать их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных;
- убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных;
- принимать необходимые правовые, организационные и технические меры или обеспечивать 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;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;
- разъяснять субъекту персональных данных юридические последствия отказа предоставить его персональные данные, а также порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставлять возможность заявить возражение против такого решения, а также разъяснять порядок защиты субъектом персональных данных своих прав и законных интересов;

- не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено ФЗ «О персональных данных»;
- принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Общество самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено данным ФЗ «О персональных данных» или другими федеральными законами.

Общество несет иные обязанности, установленные ФЗ «О персональных данных».

1.3.2 Права и обязанности субъекта персональных данных

Субъект персональных данных Общества имеет право:

- обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;
- требовать от оператора уточнения его 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;
- принимать решение о предоставлении своих персональных данных оператору и давать согласие на их обработку свободно, своей волей и в своем интересе или отзывать свое согласие на обработку персональных данных;
- на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
 - а) подтверждение факта обработки персональных данных оператором;
 - б) правовые основания и цели обработки персональных данных;
 - в) цели и применяемые Обществом способы обработки персональных данных;
 - г) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании ФЗ «О персональных данных»;
 - д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен ФЗ «О персональных данных»;
 - е) сроки обработки персональных данных, в том числе сроки их хранения;
 - ж) порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ «О персональных данных»;
 - з) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- и) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу;
- к) иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

Право субъекта персональных данных на получение информации, касающейся обработки его персональных данных, может быть ограничено в случаях, установленных ФЗ «О персональных данных».

Субъект персональных данных имеет также иные права, установленные ФЗ «О персональных данных».

Субъект персональных данных Общества обязан:

- предоставлять Обществу (оператору персональных данных) точные и достоверные сведения о своих персональных данных в объеме, определяемом целями обработки персональных данных;
- в случае изменения персональных данных оперативно сообщать об этом представителям Общества, занимающихся их обработкой;
- взаимодействовать с Обществом по вопросам обработки и защиты его персональных данных в соответствии с требованиями законодательства Российской Федерации, нормативных актов органов исполнительной власти и внутренними документами Общества.

2. Цели обработки персональных данных субъектов персональных данных Общества

Общество осуществляет обработку персональных данных в следующих целях:

- обеспечения доступа клиентов к соответствующим услугам Общества, осуществляемым Обществом в рамках лицензируемых видов деятельности, а также к сопутствующим сервисам Общества;
- осуществления исполнения заключенных договоров с физическими лицами, состоящими в договорных и иных гражданско – правовых отношениях с Обществом;
- обеспечения выполнения договорных отношений с работником, а также в других целях, предусмотренных Уставом Общества и иными внутренними документами Общества.

Обработка и хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных. Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Состав обрабатываемых в Обществе персональных данных, а также цели и правовые основания такой обработки определены в законах и иных нормативных правовых актах, в договорах с субъектом персональных данных, а также в других источниках.

Содержание и объем обрабатываемых персональных данных не должны быть избыточными по отношению к заявленным целям их обработки.

3. Категории обрабатываемых персональных данных, категории субъектов персональных данных

3.1. Категории обрабатываемых персональных данных.

В Обществе в соответствии с ФЗ «О персональных данных» выделяются следующие категории персональных данные:

- персональные данные категории «**иные**», которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным;
- **обезличенные** и/или **общедоступные** персональные данные.

Вышеуказанные категории персональных данных классифицированы Обществом с учетом степени тяжести последствий потери свойств безопасности персональных данных для субъекта персональных данных. Эти категории персональных данных могут обрабатываться как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных категории **специальные**, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, а также категории **биометрические** - в Обществе не осуществляется.

3.2. Категории субъектов персональных данных

В качестве субъектов персональных данных, персональные данные которых могут обрабатываться и соответственно защищаться в Обществе с использованием или без использования средств автоматизации, понимаются нижеперечисленные категории физических лиц, условно именуемые далее:

- а) **клиентами**, в состав которых включаются:
 - руководители, представители и работники юридических лиц, заключивших договоры с Обществом о предоставлении клиринговых услуг, а также услуг по проведению организованных торгов (других видов услуг) или находящихся на этапе преддоговорных отношений с Обществом;
- б) **работниками**, в состав которых включаются:
 - персонал Общества (работники, имеющие трудовые отношения с Обществом), кандидаты на работу в Обществе и лица, имевшие ранее трудовые отношения с Обществом;
 - лица, имеющие гражданско-правовые договоры с Обществом или находящиеся на этапе преддоговорных отношений подобного характера;
 - лица, проходящие различного рода практику (стажировку) в Обществе.
- в) **иными субъектами персональных данных**, которые не вошли в вышеперечисленные категории и обработка персональных данных которых не противоречит законодательству Российской Федерации, в т. ч.:
 - акционеры;
 - члены Совета директоров;

- лица, указанные в бюллетенях для голосования в качестве кандидатов в члены в Совет директоров, Ревизионную комиссию, членов Совета секций.

4. Порядок и условия обработки персональных данных

4.1. Перечень действий, совершаемых Обществом с персональными данными субъектов персональных данных и способы их обработки

Общество обрабатывает персональные данные субъектов персональных данных, без использования средств автоматизации. Перечень действий, совершаемых Обществом, как оператором персональных данных включает в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных всех категорий субъектов персональных данных.

Уточнение (обновление, изменение) или актуализация (исправление) персональных данных субъектов персональных данных осуществляется в случае подтверждения неточности персональных данных или выявления случая неправомерности их обработки. В этом случае их обработка блокируется и выполняются действия, определенные внутренними документами Общества.

Уничтожение (удаление) персональных данных осуществляется Обществом при достижении цели обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому выступает субъект персональных данных;
- Общество не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных ФЗ «О персональных данных»;
- иное не предусмотрено иным соглашением между Обществом и субъектом персональных данных.

4.2. Передача персональных данных субъектов персональных данных третьим лицам

Передача третьим лицам персональных данных субъектов персональных данных осуществляется только с письменного согласия таких субъектов, которое оформляется по форме, утвержденной внутренними документами Общества, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъектов, а также в случаях, установленных федеральными законами Российской Федерации.

Если персональные данные субъектов персональных данных передаются третьим лицам с целью выполнения договора между Обществом и лицом, которому передаются персональные данные, то в таком договоре должны содержаться обязательства сторон по обеспечению конфиденциальности и безопасности обрабатываемых персональных данных.

Обществом и третьими лицами, получающими доступ к персональным данным работников, обеспечивается конфиденциальность таких данных на основании Соглашения об обеспечении безопасности персональных данных, за исключением:

- обезличенных персональных данных;

– общедоступных персональных данных.

Общество вправе получать персональные данные субъектов персональных данных от третьих лиц только при наличии письменного согласия субъекта, при этом Общество должно сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере, подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

В случае если договор был заключен до вступления в силу ФЗ «О персональных данных», либо условие конфиденциальности персональных данных не было включено по каким-либо причинам, необходимо подписывать дополнительное соглашение о неразглашении персональных данных. Соглашение о неразглашении персональных данных должно быть подписано до момента передачи персональных данных.

Информация, относящаяся к персональным данным субъектов персональных данных, может быть предоставлена государственным органам в порядке, установленном федеральным законодательством Российской Федерации.

Общество не может сообщать персональные данные субъектов персональных данных в коммерческих целях без их письменного согласия.

Общество может передавать персональные данные работника его представителям в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Трансграничная передача персональных данных в Обществе осуществляется в случаях, предусмотренных законодательством Российской Федерации.

4.3. Условия прекращения обработки персональных данных

Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъектами персональных данных, а также выявление неправомерности обработки персональных данных оператором (Обществом).

Прекращение обработки персональных данных по перечисленным выше обстоятельствам осуществляется с использованием форм документов, определенных во внутренних документах Общества.

4.4. Порядок хранения персональных данных

Хранение персональных данных субъектов персональных данных осуществляется Обществом в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Хранение персональных данных осуществляется как на бумажных носителях, так и в виде электронных документов в соответствующих базах данных.

Сроки хранения определяются законодательством Российской Федерации, нормативными актами исполнительных органов государственной власти.

5. Защита персональных данных в Обществе, обеспечение безопасной обработки персональных данных

С целью обеспечения защиты законных интересов субъектов персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий, в Обществе разработана, внедрена и поддерживается в работоспособном состоянии система защиты персональных данных, которая является частью информационной инфраструктуры Общества.

Применение правовых, организационных и технических решений в соответствии со статьей 19 ФЗ «О персональных данных» по обеспечению безопасности персональных данных при их обработке включает в себя:

- утверждение Обществом внутренних документов, определяющих политику Общества в отношении обработки персональных данных, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- определение актуальности угроз безопасности персональным данным при их обработке в ИСПДн;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;
- назначение лица, ответственного за организацию обработки персональных данных;
- назначение администратора безопасности персональных данных для каждой ИСПДн, находящейся в эксплуатации;
- выполнение организационно-технических мероприятий по предотвращению фактов несанкционированного доступа к персональным данным с целью их модификации, уничтожения и распространения, определения уровня защищенности персональных данных, установленного нормативными правовыми актами Правительства Российской Федерации, для обеспечения защиты персональных данных;
- применение, прошедших в установленном порядке процедуру оценки соответствия, средств защиты информации;
- установление правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечения регистрации и учета действий, совершаемых с персональными данными в ИСПДн;
- использование процедур архивирования для восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление режима конфиденциальности в Обществе для обеспечения безопасности обработки персональных данных;
- ознакомление работников Общества, непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных и обучение работников;

- проведение самооценки, осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Общества, внутренним документам Общества в отношении обработки персональных данных.

6. Ответственность

Работники, выполняющие процедуры обработки персональных данных поддержки функционирования ИСПДн, обеспечения защиты персональных данных, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей в пределах, определенных законодательством Российской Федерации, внутренними документами Общества.