

**Общество с ограниченной ответственностью  
«ББР БРОКЕР»**

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Генеральный директор  ООО «ББР БРОКЕР»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.М. Бичурин  «14» июля 2022 г. |

**Политика обработки персональных данных**

С изменениями от 27.10.2022

Санкт-Петербург,

2022

# Оглавление

[1. Общие положения 3](#_Toc88635659)

[2. Персональные данные 4](#_Toc88635660)

[3. Организация обработки персональных данных 5](#_Toc88635661)

[3.1. Принципы обработки персональных данных. 5](#_Toc88635662)

[3.2. Права и обязанности сторон. 6](#_Toc88635663)

[3.3. Право Субъекта на получение сведений об обработке персональных данных. 6](#_Toc88635664)

[3.4. Право Субъекта на уточнение, блокирование и уничтожение данных. 8](#_Toc88635665)

[4. Цели обработки персональных данных 9](#_Toc88635666)

[5. Требования к обработке персональных данных 12](#_Toc88635667)

[5.1. Поручение на обработку персональных данных. 12](#_Toc88635668)

[5.2. Сбор персональных данных и согласие на обработку. 13](#_Toc88635669)

[5.3. Уточнение персональных данных. 14](#_Toc88635670)

[5.4. Отзыв согласия на обработку. 15](#_Toc88635671)

[5.5. Обработка без использования средств автоматизации. 15](#_Toc88635672)

[5.6. Передача (распространение). 16](#_Toc88635673)

[5.7. Сроки обработки и уничтожения. 17](#_Toc88635674)

[5.8. Устранение нарушений при обработке персональных данных. 17](#_Toc88635675)

[5.9. Приём обращений Субъектов. 18](#_Toc88635676)

[6. Защита персональных данных 19](#_Toc88635677)

# 1. Общие положения

**1.1**. Настоящая Политика обработки персональных данных является внутренним документом ООО «ББР БРОКЕР», определяющим его политику в отношении обработки персональных данных исходя из характера и масштаба деятельности.

**1.2**. Для целей Политики используются следующие термины и определения:

**Архивный перечень** – утверждённый федеральным органом исполнительной власти, осуществляющим функции по регулированию в сфере архивного дела, перечень архивных документов, образующихся в деятельности организаций, с указанием сроков их хранения.

**Клиент** – любое лицо, вне зависимости от организационно-правовой формы, заключившее (планирующее заключить) с Организаций договор (совершить иные действия, приравненные к заключению договора).

**Контролёр** – сотрудник Организации, исполняющий функции внутреннего контролёра в соответствии с Указанием Банка России № 5683-У от 28.12.2020 «О требованиях к системе внутреннего контроля профессионального участника рынка ценных бумаг».

**Нормативные требования** – обязательные для исполнения Организацией, её органами управления или служащими требования законодательства, нормативных правовых актов, Устава, внутренних нормативных и организационно-распорядительных документов Организации, базовых стандартов и стандартов саморегулируемых организаций, иных документов.

**Организация** – ООО «ББР БРОКЕР».

**Субъект** – субъект персональных данных, лицо (лицо, определяемое на основании персональных данных).

**Закон № 152-ФЗ** – Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных».

**1.3**. Организация обрабатывает персональные данные в составе и в целях, определённых Разделом 4.

**1.4**. Лицом, ответственным за организацию обработки персональных данных в Организации, является системный администратор, который получает указания непосредственно от Генерального директора и подотчётен ему. Системный администратор:

* осуществляет внутренний контроль за соблюдением Организацией и её работниками законодательства России о персональных данных, в том числе требований к защите персональных данных;
* доводит до сведения работников Организации положения законодательства России о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
* организовывает приём и обработку обращений и запросов субъектов персональных данных или их представителей.

**1.5**. Сведения об Организации и лице, ответственным за организацию обработки персональных данных вносятся по заявлению Организации в Реестр операторов, осуществляющих обработку персональных данных, размещённый на сайте Роскомнадзора.

Ответственность за актуализацию сведений несёт Генеральный директор.

**1.6**. Политика раскрывается на сайте Организации, в том числе на страницах сайта, с использованием которых осуществляется сбор персональных данных, не позднее рабочего дня, следующего за днём утверждения новой редакции (внесения изменений).

Ответственность за раскрытие возлагается на лицо, ответственное за актуализацию информации на сайте Организации. Ответственность за направление указанному лицу документа, подлежащего раскрытию, возлагается на Контролёра.

**1.7**. Функции, возлагаемые Политикой на работников Организации, исполняются сотрудниками, постоянно или временно занимающими соответствующие должности.

Обязанности, права и функции, Субъекта, предоставленные ему Политикой или нормативными требованиями, могут быть реализованы им самим или его уполномоченным представителем. В последнем случаи в распоряжении Организации должен быть предоставлен документ, подтверждающий полномочия представителя (в оригинале или нотариально заверенной копии). Организация также вправе самостоятельно изготовить копию с такого документа и хранить её наравне с оригиналом.

**1.8**. Указание на пункты, разделы и Приложения в Политике являются ссылками на пункты, разделы и Приложения к самой Политике.

**1.9.** Ответственность за актуализацию Политики возлагается на Контролёра.

# 2. Персональные данные

**2.1**. Персональные данные - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу.

Организация обрабатывает следующие виды данных: собственно персональные данные, обезличенные, специальные и биометрические персональные данные. Вид данных определяет требования к порядку обработки и защиты информации.

Под обработкой понимается любое действие или операция (их совокупность), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.1.1. Так как законодательство не определяет закрытый перечень сведений, которые относятся к персональным данным, персональными данными считается любой возможный набор сведений (информации, данных), который позволяет с уверенность выделить физическое лицо из множества иных лиц.

2.1.2. Обезличенные персональные данные –данные, на основании которых прямо или косвенно определить физическое лицо возможно только при использовании дополнительной информации.

Обезличивание персональных данных не является процессом, который превращает персональные данные в обычные данные (не делает данные анонимными), так как у Организации или третьего лица сохраняется возможность «обратной идентификации» при использовании иной информации. Для определения того, является ли набор сведений анонимными данными или обезличенными персональными данными, Организация руководствуется следующим:

**А**. Если у Организации нет доступа (возможности доступа) к дополнительной информации, использование которой позволяет прямо или косвенно определить физическое лицо (провести обратную идентификацию) – информация считается анонимными данными и не считается обезличенными персональными данными.

**Б**. Если Организация имеет или может получить доступ к дополнительной информации из внешних источников – она считается имеющей доступ к дополнительной информации.

**В**. Если доступ к дополнительным источникам информации для Организации возможен только с нарушением законодательства (путём участия в отношениях, связанных с таким нарушением) – Организация считается не имеющей доступа к такой информации.

**Г**. Шифрование информации и ограничение к ней доступа никак не влияет на признание информации анонимными данными, однако может быть основанием для признания персональных данных обезличенными.

2.1.3. Специальные персональные данные – персональные данные, дополненные информацией, касающиеся расовой или национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

2.1.4. Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

**2.2**. Организация обрабатывает персональные данные в соответствии с принципами, указанными в п.3.1.

2.2.1. Порядок обработки персональных данных определяется Организацией самостоятельно, исходя из имеющихся в её распоряжении ресурсов и применяемых порядков осуществления операций, внутреннего контроля и защиты информации.

2.2.2. Вне зависимости от того, использует ли Организация для обработки персональных данных системы автоматизации, персональные данные подразделяются на:

* обрабатываемые без использования средств автоматизации и
* обрабатываемые с использованием средств автоматизации.

Персональные данные считают обрабатываемыми без использования средств автоматизации, если их использование, уточнение, распространение, уничтожение осуществляется при непосредственном участии сотрудника Организации. Тот факт, что данные хранятся или извлекаются из информационной системы, не влияет на факт признания обработки без использования средств автоматизации.

Иные данные считаются обрабатываемыми с использованием средств автоматизации.

Вид обработки персональных данных определяет требования к обработке, включая требования к применяемым типовым формам документации.

# 3. Организация обработки персональных данных

## 3.1. Принципы обработки персональных данных.

3.1.1. Обработка персональных данных осуществляется на законной и справедливой основе и ограничивается достижением конкретных и законных целей, определённых Разделом 4.

3.1.2. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.1.3. Не допускается обработка персональных данных, несовместимых с целями сбора и обработки персональных данных. Если Организация каким-либо образом получила персональные данные, не соответствующие целям обработки, сотрудник, принявший (обнаруживших) указанные данные, должен уничтожить их в порядке, определённом п.5.7.

3.1.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Решение о том, совместимы ли цели, принимается Контролёром.

3.1.5. Базы данных, используемые Организацией для обработки персональных данных, располагаются на территории России.

3.1.6. При обработке персональных данных должны быть обеспечены их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки.

Если Организация признаёт данные неполными или неточными, такие данные уточняются в соответствии с п.5.3 или удаляются без обработки в соответствии с п.5.7.

3.1.7. Организация обеспечивает конфиденциальность и защиту персональных данных в соответствии с Разделом 6.

3.1.8. Хранение персональных данных осуществляется в форме, позволяющей определить Субъекта, не дольше, чем этого требуют цели обработки, если срок хранения не установлен федеральным законом, договором, стороной, выгодоприобретателем или поручителем по которому является Субъект.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении целей, если иное не предусмотрено федеральным законом.

3.1.9. Организация (её сотрудники, лица, которым поручена обработка персональных данных) не раскрывает третьим лицам персональные данные без согласия Субъекта, если иное не предусмотрено федеральным законом.

Организация не распространяет персональные данные Субъекта, исключая случаи, когда необходимость распространения прямо предусмотрена законодательством.

3.1.10. Организация на основании исключительно автоматизированной обработки персональных данных не принимает решений, порождающих юридические последствия в отношении Субъекта или иным образом затрагивающих его права и законные интересы.

## 3.2. Права и обязанности сторон.

3.2.1. Организация как оператор персональных данных, вправе:

* отстаивать свои интересы в суде;
* предоставлять персональные данные Субъекта иным лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
* отказывать в предоставлении персональных данных, в случаях, предусмотренных законодательством;
* использовать персональные данные Субъекта без его согласия, в случаях, предусмотренных законодательством.

3.2.2. Организация как оператор персональных данных, обязана:

* предоставлять Субъекту по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставить отказ (п.3.3);
* по требованию Субъекта уточнять обрабатываемые персональные данные, блокировать их или удалять, если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки (п.3.4, 5.8);
* уведомлять Субъекта об обработке персональных данных если персональные данные были получены не от Субъекта (п.3.3.4);
* прекратить обработку персональных данных и уничтожить их (п.5.7).

3.2.3. Субъект имеет право:

* требовать уточнения своих данных, их блокирования или уничтожения если данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
* требовать перечень своих персональных данных, обрабатываемых Организацией и источник их получения;
* получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
* требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
* обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;
* на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3.2.4. Субъект обязан:

* своевременно и точно предоставлять персональные данные, необходимые Организации для исполнения обязательств перед Субъектом;
* уведомлять Организацию об изменении сведений, содержащих персональные данные, в порядке, составе и в срок, определённый договорами между Организацией и Субъектом.

## 3.3. Право Субъекта на получение сведений об обработке персональных данных.

3.3.1. Организация обязана безвозмездно предоставить Субъекту информацию, указанную ниже, в случаях, предусмотренных п.3.3.2 – 3.3.3:

* подтверждение факта обработки персональных данных Организацией;
* правовые основания и цели обработки персональных данных;
* цели и применяемые Организацией способы обработки персональных данных;
* наименование и место нахождения Организации, сведения о лицах (за исключением работников Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Организацией или на основании федерального закона;
* обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
* сроки обработки персональных данных, в том числе сроки их хранения;
* порядок осуществления субъектом персональных данных прав, предусмотренных Законом № 152-ФЗ;
* информацию об осуществленной или о предполагаемой трансграничной передаче данных;
* наименование (фамилию, имя, отчество) и адрес лица, осуществляющего обработку персональных данных по поручению Организации, если обработка поручена или будет поручена такому лицу;
* информацию о способах исполнении Организацией обязанностей, установленных ст.18.1 Закона № 152-ФЗ;
* иные сведения, предусмотренные Законом № 152-ФЗ или другими федеральными законами.

3.3.2. Субъект (если иное не следует из законодательства) вправе направить Организации запрос об обработке персональных данных, содержащий указание на предоставление Субъекту информации, обрабатываемой Организацией. Запрос должен содержать:

* номер, дату выдачи, орган, выдавший основной документ, удостоверяющий личность Субъекта (его представителя),
* сведения, подтверждающие участие Субъекта в отношениях с Организацией (номер и дата заключения договора, условное словесное обозначение, иные сведения), или иное подтверждение факта обработки персональных данных Организацией,
* подпись Субъекта (его представителя),
* обоснование направление повторного запроса (при направлении повторного запроса в течение 30 дней от даты направления идентичного запроса).

3.3.2.1. Запрос регистрируется в соответствии с п.5.9 и направляется Контролёру, который контролирует наличие следующих оснований для отказа в предоставлении информации:

А. Запрос не содержит сведения, указанные выше.

Б. У Организации отсутствуют документы, подтверждающие полномочия представителя, подписавшего запрос.

В. Менее 30 дней назад Организации уже был направлен идентичный запрос. Исключением являются случаи, когда:

* более короткий срок установлен Законом № 152-ФЗ (принятыми в соответствии с ним нормативными актами), договором, стороной (выгодоприобретателем, поручителем) по которому является Субъект,
* Организация не предоставила Субъекту его данные для ознакомления в полном объёме по результатам рассмотрения первоначального обращения.

3.3.2.2. При наличии достаточных обоснований для отказа от исполнения запроса, Контролёр направляет подателю запроса мотивированный отказ с указанием оснований и ссылок на положения ч.8 ст.14 Закона № 152-ФЗ (иного федерального закона).

Отказ направляется по реквизитам, указанным в запросе, не позднее 30 дней от даты получения запроса Субъекта.

Копия отказа помещается в дела Контролёра совместно с ненадлежащим запросом, где и хранится.

3.3.2.3. При отсутствии оснований для отказа, Контролёр направляет способом, указанным в запросе, информацию в доступной форме, не содержащую персональных данных иных субъектов (исключая случаи наличия законных оснований для раскрытия таких данных). Информация предоставляется не позднее 30 дней от даты получения запроса.

3.3.3. Субъект вправе запросить информацию об обработке персональных данных при сборе персональных данных Организацией.

Если запрос представлен в письменном виде, он регистрируется в порядке, предусмотренном п.5.9.

Информация предоставляется лицом, осуществляющим сбор персональных данных, самостоятельности либо при участии Контролёра.

3.3.4. Если персональные данные получены не от Субъекта, Организация до начала обработки персональных данных предоставляет Субъекту:

* наименование и адрес Организации;
* цель обработки персональных данных и ее правовое основание;
* предполагаемые пользователи персональных данных;
* установленные Законом № 152-ФЗ права субъекта персональных данных;
* перечень персональных данных;
* источник получения персональных данных.

Исключением являются случаи, когда:

* Субъект уведомлен об осуществлении обработки его персональных данных иным оператором;
* персональные данные получены Организацией на основании федерального закона или в связи с исполнением договора, стороной (выгодоприобретателем, поручителем) по которому является Субъект;
* предоставление Субъекту сведений нарушает права и законные интересы иных лиц.

## 3.4. Право Субъекта на уточнение, блокирование и уничтожение данных.

3.4.1. Субъект вправе требовать от Организации уточнения его персональных данных, их блокирования или уничтожения если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Субъект также вправе требовать от Организации принятия предусмотренных законом мер по защите своих прав.

3.4.2. Указанное требование оформляется и регистрируется аналогично запросу о предоставлении сведений в соответствии с п.3.3.2.

При необходимости уточнения персональных данных к требованию должны быть приложены документы, подтверждающие достоверность сведений, требующих уточнения.

3.4.3. Требование направляется Контролёру, который контролирует наличие оснований для отказа от исполнения требования, к которым относятся:

А. Запрос не содержит сведения, указанные в п.3.3.2.

Б. У Организации отсутствуют документы, подтверждающие полномочия представителя, подписавшего запрос.

В. У Организации отсутствуют основания для реализации действий, предусмотренных требованием.

3.4.4. При отсутствии оснований для отказа от исполнения Контролёр организует мероприятия по его исполнению, при необходимости – направляя иным подразделениям и должностным лицам Организации требование и приложенные к нему документы.

Контролёр информирует подателя требования о результатах его исполнения только если такая необходимость прямо предусмотрена требованием.

3.4.5. Требование, ответы и иные сопутствующие документы хранятся в документах Контролёра.

# 4. Цели обработки персональных данных

**4.1**. Организация обрабатывает персональные цели только для достижения целей, указанных в настоящем Разделе. Если по каким-либо причинам Организация получает персональные данные, не являющиеся необходимыми для достижения заявленных целей, Организация обеспечивает их уничтожение в соответствии с п.5.7 – 5.8.

**I. Цель обработки**: контроль над соответствием лица требованиям к опыту работы, репутации и квалификации, предъявляемым законодательством о деятельности финансовых организаций.

**Категории персональных данных**: персональные данные, не относящиеся к биометрическим, специальные персональные данные об отсутствии судимости, дисквалификации или запрета на занятие отдельных должностей.

**Перечень персональных данных**:

* фамилия, имя, отчество,
* гражданство, налоговое резидентство, налоговые и иные присвоенные лицу государственным органом идентификаторы,
* регистрационные данные удостоверения личности,
* данные адреса места жительства, места пребывания, контактный адрес,
* данные о трудовой деятельности: занимаемые должности и места работы,
* данные о владении (наличии права распоряжаться) долями в капитале юридических лиц,
* данные об образовании, переподготовке, специальной квалификации,
* данные о судимости, дисквалификации или запрете на занятие отдельных должностей.

**Субъекты персональных данных**: лица, которых Организация планирует назначить или избрать (в том числе – временно) на должности (в состав органов), к которым законодательством о финансовых организациях предусмотрены требования о квалификации или деловой репутации.

**Способы обработки**: без использования средств автоматизации.

**Сроки обработки и хранения**: от момента предоставления персональных данных Субъектом до момента истечения срока хранения, предусмотренного Архивным перечнем. По лицам, не назначенным (не избранным) на должности (в состав органов) – в течение одного календарного месяца от даты соответствующего решения.

**II. Цель обработки**: контроль над соответствием лица требованиям к опыту работы и квалификации, предъявляемым Организацией.

**Категории персональных данных**: персональные данные, не относящиеся к биометрическим или специальным.

**Перечень персональных данных**:

* фамилия, имя, отчество,
* регистрационные данные удостоверения личности,
* данные о трудовой деятельности: занимаемые должности и места работы,
* данные об образовании, переподготовке, специальной квалификации.

**Субъекты персональных данных**: кандидаты на занятие должностей в Организации.

**Способы обработки**: без использования средств автоматизации.

**Сроки обработки и хранения**: от момента предоставления персональных данных Субъектом до момента истечения срока хранения, предусмотренного Архивным перечнем. По лицам, не назначенным (не избранным) на должности (в состав органов) – в течение одного календарного месяца от даты соответствующего решения.

**III. Цель обработки**: заключение и исполнение трудовых договоров, исполнение обязанностей, возложенных на Организацию законодательством о труде, социальной защите, пенсионном обеспечении, обязательном страховании и воинском учёте.

**Категории персональных данных**: персональные данные, за исключением биометрических персональных данных.

**Перечень персональных данных**:

* фамилия, имя, отчество,
* гражданство, налоговое резидентство, налоговые и иные присвоенные лицу государственным органом идентификаторы и статусы,
* регистрационные данные удостоверения личности,
* регистрационные данные удостоверения о воинском учёте,
* данные адреса места жительства, места пребывания, контактный адрес,
* данные о трудовой деятельности: занимаемые должности и места работы,
* данные об образовании, переподготовке, специальной квалификации,
* данные о воинском звании, прохождении воинской службы, учётной специальности, мобилизационной категории,
* данные о государственных наградах и званиях,
* данные, подтверждающие право на дополнительный отпуск, выплаты, совершение отдельных кадровых действий и мероприятий,
* данные о состоянии здоровья, семейном положении, членах семьи в объёме и составе, необходимом для достижения целей обработки.

**Субъекты персональных данных**: работники Организации.

**Способы обработки**: без использования средств автоматизации.

**Сроки обработки и хранения**: от момента предоставления персональных данных Субъектом до момента истечения срока хранения, предусмотренного Архивным перечнем.

**IV. Цель обработки**: исполнение законодательства о выявлении бенефициарных владельцев Организации, учёте аффилированных лиц Организации.

**Категории персональных данных**: персональные данные, не относящиеся к биометрическим или специальным.

**Перечень персональных данных**:

* фамилия, имя, отчество,
* гражданство, налоговое резидентство, налоговые и иные присвоенные лицу государственным органом идентификаторы,
* регистрационные данные удостоверения личности,
* дата и место рождения,
* данные адреса места жительства, места пребывания, контактный адрес,
* данные о владении (наличии права распоряжаться) долями в капитале юридических лиц,
* данные о составе группы лиц, к которой относится Субъект и основаниях для признания лиц группой лиц.

**Субъекты персональных данных**: члены органов управления Организации, лица, имеющие право распоряжаться долями в капитале Организации.

**Способы обработки**: без использования средств автоматизации.

**Сроки обработки и хранения**: от момента предоставления персональных данных Субъектом до момента истечения срока хранения, предусмотренного Архивным перечнем.

**V. Цель обработки**: заключение и исполнение договоров на предоставление услуг профессионального участника рынка ценных бумаг, не требующих специальной квалификации, тестирования или оценки клиента.

**Категории персональных данных**: персональные данные, не относящиеся к биометрическим или специальным.

**Перечень персональных данных**:

* фамилия, имя, отчество,
* гражданство, налоговое резидентство, налоговые идентификаторы,
* регистрационные данные удостоверения личности,
* дата и место рождения,
* данные адреса места жительства, места пребывания, контактный адрес,
* данные контактного телефона, адреса электронной почты,
* регистрационные данные документа о праве находиться в России, срок действия такого права,
* сведения о принадлежности к публичным должностным лицам,
* платёжные реквизиты (данные обслуживающих кредитных организаций, номер банковских счетов).

**Субъекты персональных данных**: клиенты Организации и лица, инициирующие заключение договоров на предоставление услуг профессионального участника рынка ценных бумаг с Организацией.

**Способы обработки**: с использованием средств автоматизации, без использования средств автоматизации.

**Сроки обработки и хранения**: от момента предоставления персональных данных Субъектом до момента истечения срока хранения, предусмотренного Архивным перечнем.

**VI. Цель обработки**: заключение и исполнение договоров на предоставление услуг профессионального участника рынка ценных бумаг, требующих специальной квалификации, тестирования или оценки клиента.

**Категории персональных данных**: персональные данные, не относящиеся к биометрическим или специальным.

**Перечень персональных данных**:

* фамилия, имя, отчество,
* гражданство, налоговое резидентство, налоговые идентификаторы,
* регистрационные данные удостоверения личности,
* дата и место рождения,
* возраст,
* сведения о величине доходов, расходов и обязательств,
* данные адреса места жительства, места пребывания, контактный адрес,
* данные контактного телефона, адреса электронной почты,
* регистрационные данные документа о праве находиться в России, срок действия такого права,
* сведения о принадлежности к публичным должностным лицам,
* платёжные реквизиты (данные обслуживающих кредитных организаций, номер банковских счетов),
* данные об образовании, наличии квалификаций,
* сведения об опыте работы с инструментами финансового рынка.

**Субъекты персональных данных**: клиенты Организации и лица, инициирующие заключение договоров на предоставление услуг профессионального участника рынка ценных бумаг с Организацией, сопровождающихся проведением квалификации, тестирования или оценки клиента.

**Способы обработки**: с использованием средств автоматизации, без использования средств автоматизации.

**Сроки обработки и хранения**: от момента предоставления персональных данных Субъектом до момента истечения срока хранения, предусмотренного Архивным перечнем.

**VII. Цель обработки**: аутентификация представителя Организации, контрагента Организации.

**Категории персональных данных**: персональные данные, не относящиеся к биометрическим или специальным.

**Перечень персональных данных**:

* фамилия, имя, отчество,
* регистрационные данные удостоверения личности.

**Субъекты персональных данных**: доверенные лица Организации, контрагентов Организации.

**Способы обработки**: без использования средств автоматизации.

**Сроки обработки и хранения**: от момента предоставления персональных данных Субъектом до момента истечения срока хранения, предусмотренного Архивным перечнем.

**VIII. Цель обработки**: составление внутренних телефонных справочников работников (не являющихся общедоступными).

**Категории персональных данных**: персональные данные, не относящиеся к биометрическим или специальным.

**Перечень персональных данных**:

* фамилия, имя, отчество,
* должность в Организации,
* внутренний телефонный номер Организации,

**Субъекты персональных данных**: работники и члены органов управления Организации.

**Способы обработки**: без использования средств автоматизации.

**Сроки обработки и хранения**: от момента приёма работника в Организацию до момента увольнения работника из Организации.

**V. Цель обработки**: исполнение Организацией требований законодательства о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком.

**Категории персональных данных**: персональные данные, не относящиеся к биометрическим или специальным.

**Перечень персональных данных**:

фамилия, имя, отчество,

дата рождения,

место рождения,

должность, которую лицо занимает в Организации.

**Субъекты персональных данных**: лица, которые в связи с заключением договора с Организацией, или в связи с назначением (избранием) в состав органов управления (контрольных органов) Организации имеют доступ к инсайдерской информации.

**Способы обработки**: без использования средств автоматизации.

**Сроки обработки и хранения**: от момента предоставления персональных данных Субъектом до момента истечения срока хранения, предусмотренного Архивным перечнем.

# 5. Требования к обработке персональных данных

## 5.1. Поручение на обработку персональных данных.

5.1.1. Организация на основании отдельного договора (если иное прямо не предусмотрено федеральным законом) вправе как поручить обработку персональных данных иному лицу, так и осуществлять такую обработку по поручению иного лица.

Решение о принятии (передаче) функций по обработке персональных данных принимает Генеральный директор при условии соблюдения условий, указанных в п.5.1.2.

5.1.2. Договор о передаче функций по обработке заключается только если одновременно:

**А**. Субъект дал согласие на такую передачу в соответствии с п.5.2.

**Б**. В договоре об обработке персональных данных указаны:

* перечень персональных данных;
* цели обработки персональных данных,
* перечень действий (операций) с персональными данные, которые будут совершаться контрагентом,
* обязанность контрагента соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством о персональных данных,
* обязанность контрагента соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке,
* требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Федерального закона № 152-ФЗ «О персональных данных».
* обязанность контрагента использовать для записи и хранения персональных данных базы данных на территории РФ;
* меры, которые должен предпринять контрагент для выполнения требований законодательства о персональных данных;
* обязанность контрагента по запросу предоставлять в течение срока действия договора информацию о соблюдении условий обработки персональных данных;
* обязанность контрагента уведомить о случаях компрометации обрабатываемых данных.

5.1.3. Если Организация обрабатывает персональные данные по поручению иного лица на основании отдельного договора, то Организация не обязана получать согласие Субъекта на обработку его данных, однако вправе требовать предоставления подтверждения законности оснований для обработки персональных данных. Ответственность за действия Организации при обработке персональных данных в соответствии с заключённым договором несёт контрагент Организации.

Если Организация поручает обработку персональных данных иному лицу, то Организация несёт ответственность перед Субъектом за действия контрагента и за подтверждение согласия Субъекта на обработку его данных третьим лицом.

5.1.4. Организация обеспечивает прекращение обработки третьим лицом, проводящим обработку персональных данных, при наступлении сроков завершения обработки в соответствии с п.5.7.

## 5.2. Сбор персональных данных и согласие на обработку.

5.2.1. Если обработка персональных данных (исключая специальные и биометрические персональные данные) не связана с:

* необходимостью достижения целей, предусмотренных международным договором Российской Федерации или законом,
* выполнением возложенных законодательством России на Организацию функций, полномочий и обязанностей,
* участием Организации в судопроизводстве и исполнительном производстве,
* заключением договора[[1]](#footnote-1) по инициативе Субъекта,
* заключением договора, где Субъект будет выгодоприобретателем или поручителем,
* необходимостью исполнения договора стороной, выгодоприобретателем или поручителем по которому является Субъект,
* необходимостью защиты жизни, здоровья или иных жизненно важных интересов Субъекта и получение его согласия невозможно,
* необходимостью осуществления прав и законных интересов Организации или третьих лиц (при условии не нарушения прав и свободы Субъекта),
* необходимостью опубликования или обязательного раскрытия данных в соответствии с федеральным законом.

Организация обязана получить у Субъекта (включая работника Организации) предварительное согласие. Форма согласия должна содержать:

* в отношении Субъекта (представителя, подписавшего согласие) - фамилию, имя, отчество, адрес, номер основного документа, удостоверяющего личность, сведения о дате выдачи и выдавшем его органе;
* если согласие дано представителем – дополнительно указываются реквизиты доверенности или иного документа, подтверждающего полномочия представителя,
* наименование и адрес Организации;
* цель обработки персональных данных;
* перечень персональных данных, на обработку которых дается согласие;
* если обработка будет поручена иному лицу – его наименование (фамилия, имя, отчество) и адрес;
* перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
* срок, в течение которого действует согласие,
* способ отзыва согласия, если иное не установлено федеральным законом;
* подпись Субъекта (его представителя).

Если в соответствии предоставление персональных данных и (или) получение Организацией согласия на обработку персональных данных являются обязательными, Организация обязана разъяснить Субъекту юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

5.2.2. Организация обрабатывает специальные персональные данные только:

* в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством России;
* если обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта (иных лиц) и получить согласие Субъекта невозможно;
* если обработка необходима для установления или осуществления прав Субъекта или третьих лиц, а равно и в связи с осуществлением правосудия;
* обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

Обработка специальных персональных данных в вышеуказанных случаях не требует получение согласия Субъекта.

5.2.3. Если Организация использует биометрические персональные данные для установления личности Субъекта, обработка таких персональных данных производится только при условии получения Организацией предварительного согласия на обработку персональных данных.

Если же биометрические персональные данные используются для подтверждения совершения Субъектом определённого действия (заключения договора, отдачи поручения и т.п.) – согласие на обработку подобных данных не требуется.

5.2.4. Согласие на обработку может быть предоставлено самим Субъектом либо его уполномоченным представителем. В последнем случае лицо, получающее согласие в соответствии с п.5.2.5, приобщает к согласию оригинал или копию документа, подтверждающего полномочия представителя.

5.2.5. Согласие на обработку персональных данных получает подразделением (должностным лицом), осуществляющим обработку получаемых персональных данных в соответствии с внутренними документами Организации.

Если получение согласия сопровождалось заключением договора, стороной, выгодоприобретателем или поручителем по которому является Субъект – согласие хранится совместно с договором. Копии согласия могут предоставляться иным подразделениям и должностным лицам, если они также обрабатывают персональные данные в целях, заявленных в согласии.

В противном случае согласие хранится в подразделении, получившем согласие, в течение сроков обработки персональных данных, указанных в согласии.

## 5.3. Уточнение персональных данных.

5.3.1. Организация утверждает в составе типовых договоров требование о необходимости обновления персональных данных Субъектами при утере актуальности.

Сроки, порядок и состав указанных данных определяется в соответствии с требованиями законодательства, учитываемыми при определении целей обработки персональных данных.

Одновременно, в случаях, когда это предусмотрено требованиями законодательства, Организация контролирует актуальность персональных данных и при выявлении достаточных оснований считать персональные данные утратившими актуальность уведомляет Субъекта о необходимости уточнения персональных данных.

5.3.2. Если Организация признаёт персональные данные утратившими актуальность, обработка таких данных приостанавливается, исключая обработку в целях уточнения и хранения персональных данных. В ряде случаев, предусмотренных законодательством и внутренними нормативными документами такая приостановка влечёт необходимость отказа Организации от обслуживания Субъекта.

5.3.3. Уточнение персональных данных производится путём предоставления Субъектов документов, свидетельствующих об изменении персональных данных (копий удостоверений личности, заявлений об изменении и т.п.).

Субъект также вправе направить Организации требование об уточнении персональных данных в соответствии с п.3.4.

5.3.4. Документы, подтверждающие необходимость уточнения персональных данных, передаются подразделению (должностному лицу), осуществляющему ведение документов, фиксирующих персональные данные, или ответственному за актуализацию персональных данных в информационных системах.

5.3.5. Уточнение персональных данных и прекращение их блокирования производится не позднее 7 рабочих дней от даты предоставления актуальных сведений. Если обработка персональных данных производится по поручению Организации иным лицом – Организация обязана обеспечить соблюдение вышеуказанных сроков.

5.3.6. Уточнение персональных данных, хранящихся в информационных системах, производится путём изменения информации с одновременным обеспечением возможности получение персональных данных Субъекта на любую дату, в которую осуществлялась обработка персональных данных Субъекта.

Отдельные особенности уточнения персональных данных без использования средств автоматизации указаны в п.5.5.

## 5.4. Отзыв согласия на обработку.

5.4.1. Субъект вправе представить Организации в свободной форме заявление на отзыв согласия на обработку.

Форма заявления должно позволить идентифицировать лицо, подающее заявление, и Субъект, согласие которого отзывается.

5.4.2. Заявление передаётся должностному лицу (подразделению), осуществляющему обработку персональных данных Субъекта (при наличии – в сопровождении оригинала или копии документа, подтверждающего полномочия представителя Субъекта).

5.4.3. Получатель заявления контролирует наличие основания для прекращения обработки персональных данных и, при наличии, прекращает такую обработку в соответствии с п.5.7.

Даже при отзыве согласия на обработку персональных данных Организация продолжает обрабатывать персональные данные Субъекта, если для такой обработки в соответствии с требованием законодательства не требуется получение согласия.

## 5.5. Обработка без использования средств автоматизации.

Если данные обрабатываются без использования средств автоматизации,

5.5.1. Каждый сотрудник Организации в порядке, определённом должностными инструкциями и внутренними нормативными документами, участвует в обработке персональных данных без использования средств автоматизации.

5.5.2. Организация использует для такой обработки отдельные формы и материальные носители, не используемые при автоматической обработке информации.

5.5.3. При обработке Организация обособляет персональные данные от иной информации и использует разные материальные носители для персональных данных, цели обработки которых заведомо несовместимы или относятся к различным категориям персональных данных (включая запрет на объединение полей формы).

5.5.4. Типовые формы, характер которых предполагает или допускает включение в них персональных данных, утверждается с учётом следующего:

**А**. Типовая форма или связанные с ней документы[[2]](#footnote-2) (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:

* сведения о цели обработки персональных данных
* наименование и адрес Организации,
* фамилию, имя, отчество и адрес Субъекта,
* источник получения персональных данных,
* сроки обработки персональных данных,
* перечень действий с персональными данными, которые будут совершаться в процессе их обработки,
* общее описание используемых Организацией способов обработки персональных данных.

**Б**. Если получение персональных данных сопровождается необходимостью получения предварительного согласия в соответствии с п.5.2 - типовая форма должна предусматривать поле, в котором Субъект может поставить отметку о своем согласии.

**В**. Если типовая форма предусматривает указание персональных данных нескольких субъектов – форма составляется так, чтобы каждый из заполняющих форму имел возможность ознакомиться со своими персональными данными в форме не нарушая прав и законных интересов иных субъектов персональных данных.

5.5.5. При несовместимости целей обработки данных, зафиксированных на одном материальном носителе, если носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, Организация:

**А**. При необходимости отдельного использования или распространения определенных персональных данных осуществляет копирование таких персональных данных способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и использует (распространяет) копию данных.

**Б**. При необходимости уничтожения или блокирования части персональных данных уничтожает или блокирует материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование данных, подлежащих уничтожению или блокированию.

5.5.6. Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это невозможно - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

## 5.6. Передача (распространение).

5.6.1. Организация передаёт и распространяет персональные данные третьим лицам только когда в соответствии с законодательством такая передача и распространение не требует получение предварительного согласия Субъекта.

5.6.2. По общим правилам, Организация не осуществляет трансграничную передачу персональных данных, однако может быть обязана осуществить такую передачу в соответствии с требованиями законодательства об иностранном налогообложении.

Если такая обязанность возникает, Организация обеспечивает соблюдение установленных законодательством России требований к обеспечению безопасности данных при передаче и получению согласия Субъекта (при передаче на территорию государств, не обеспечивающих адекватную защиту прав субъектов персональных данных).

## 5.7. Сроки обработки и уничтожения.

5.7.1. Персональные данные, обработка которых не подразумевает получения согласия на обработку в соответствии с п.5.2, обрабатываются от даты их получения до наиболее поздней из следующих дат:

* дата завершения срока хранения в соответствии с законодательством об архивном делопроизводстве (иными законодательными и нормативными актами, определяющими срок хранения персональных данных),
* дата достижения всех целей обработки персональных данных.

Если различные нормы законодательства устанавливают разные сроки хранения – Организация руководствуется наибольшим из указанных сроков.

5.7.2. Персональные данные, на обработку которых требуется согласие Субъекта, обрабатываются от даты подписания согласия до наиболее ранней из следующих дат:

* дата истечения срока обработки, указанная в согласии Субъекта,
* дата отзыва согласия Субъектом.

5.7.3. После истечения срока обработки персональных данных, они уничтожаются в течение 30 календарных дней в порядке, указанном в п.5.7.4. При невозможности соблюдения указанного срока, персональные данные блокируются на период не более, чем шесть месяцев, если иной срок не установлен федеральными законами.

Указанный срок может быть продлён соглашением с Субъектом либо договором, стороной (выгодоприобретателем, поручителем) по которому является Субъект.

Срок уничтожения персональных данных, обрабатываемых на основании согласия Субъекта, также может быть продлён если сохранение персональных данных требуется для достижения целей обработки персональных данных.

5.7.4. Уничтожение персональных данных, зафиксированных в документах, производится путём уничтожения документов способом, исключающим восстановление документа (сжигание, измельчение и т.п.). Уничтожение документов по завершении их сроков обязательного хранения в соответствии с законодательством об архивном делопроизводстве фиксируется документом за подписью лица, проводившего уничтожение.

Уничтожение персональных данных, хранящихся в информационных системах, может проводиться путём уничтожения всех носителей информации, хранящих информацию о персональных данных, путём удаления информации без возможности восстановления либо путём анонимизации данных (удаления любой дополнительной информации, позволяющей использовать сведения для прямого или косвенного определения физического лица).

Уничтожение персональных данных, обрабатываемых без использования средств автоматизации, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

5.7.5. При наступлении оснований для уничтожения (блокирования) персональных данных, обрабатываемых иным лицом по поручению Организации, Организация обеспечивает уничтожение (блокирование) данных третьим лицом в сроки, предписанные для уничтожения.

## 5.8. Устранение нарушений при обработке персональных данных.

5.8.1. При выявлении неправомерной обработки персональных данных при обращении (запросе) Субъекта или уполномоченного органа по защите прав субъектов персональных данных, Организация блокирует (обеспечивает блокирование) неправомерно обрабатываемые данные, относящихся к этому Субъекту, с момента такого обращения или получения указанного запроса на период проверки.

5.8.2. При выявлении неточных персональных данных при обращении (запросе) Субъекта или уполномоченного органа по защите прав субъектов персональных данных, Организация блокирует (обеспечивает блокирование) персональных данных, относящихся к этому Субъекту с момента такого обращения или получения указанного запроса на период проверки, если блокирование не нарушает права и законные интересы Субъекта или третьих лиц.

Уточнение персональных данных производится в соответствии с п.5.3.

5.8.3. Если персональные данные подлежат уничтожению по причине предоставления Субъектом (его представителем) подтверждения того, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Организация уничтожает соответствующие персональные данные не позднее 7 рабочих дней от даты получения подтверждения.

Дополнительно, Контролёр информирует Субъекта (его представителя) о внесённых изменения и предпринятых мерах, а также организует разумные меры по уведомлению третьих лиц, которым персональные данные этого Субъекта были переданы.

Документы, подтверждающие основания для уничтожения и направление соответствующей информации, помещаются в дела Контролёра.

5.8.4. При выявлении неправомерной обработки персональных данных Организацией (иным лицом по её поручению), Организация прекращает обработку (обеспечивает прекращение обработки) таких данных не позднее трёх рабочих дней от даты выявления такого события. Информация о прекращении направляется Контролёру.

Не позднее десяти рабочих дней от даты выявления неправомерности, Организация предпринимает все возможные действия по обеспечению правомерности обработки.

Если обеспечить правомерность обработки невозможно, Организация не позднее десяти рабочих дней от даты выявления неправомерности уничтожает персональные данные (обеспечивает их уничтожение) и информирует об этом Контролёра.

Контролёр направляет Субъекту в свободной форме уведомление об устранении допущенных нарушений или об уничтожении данных. Если выявление неправомерности сопровождалось взаимоотношениями с уполномоченными органами по защите прав субъектов персональных данных – копия уведомления направляется указанному органу.

5.8.5. При установлении факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав Субъектов, Организация обязана уведомить Роскомнадзор:

**I**. В течение 24 часов - о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав Субъектов, и предполагаемом вреде, нанесенном правам Субъектов, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав Субъектов, по вопросам, связанным с выявленным инцидентом;

**II**. В течение семидесяти двух часов - о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Отсчёт указанных сроков ведётся с момента выявления события или получения Организацией сведений о событии.

Уведомление производится Контролёром по электронным формам, размещённым на сайте Роскомнадзора.

## 5.9. Приём обращений Субъектов.

5.9.1. Обращения и запросы Субъектов регистрируются в соответствии с типовыми правилами регистрации входящих документов.

Копии указанных обращений направляются Контролёру в день их регистрации для обеспечения контроля над сроками обработки таких документов, установленными Политикой.

5.9.2. В случае обращения Субъекта к Организации с требованием о прекращении обработки персональных данных Организация в срок, не превышающий 10 рабочих дней с даты получения требования прекращает такую обработку (обеспечивает её прекращение), исключая случаи, указанные в Законе № 115-ФЗ.

# 6. Защита персональных данных

**6.1**. Персональные данные являются конфиденциальной, строго охраняемой информацией и на них распространяются все требования, установленные внутренними документами Организации к защите конфиденциальной информации. Обеспечение защиты персональных данных является одной из приоритетных задач Организации.

**6.2**. Организация проводится обучение и ознакомление работников Организации, участвующих в обработке персональных данных, с нормативными требованиями о персональных данных, в том числе с требованиями к их защите.

**6.3**. В целях обеспечения сохранности и конфиденциальности персональных данных все операции по обработке персональных данных выполняются только работниками подразделений, которым указанные данные необходимы для достижения целей обработки персональных данных, функции и обязанности которых регулируются их должностными инструкциями и внутренними нормативными документами.

**6.4**. Ответы на запросы, подразумевающие предоставление персональных данных, предоставляются в объёме, который позволяет не разглашать излишний объем персональных сведений.

**6.5**. Материальные носители персональных данных хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

**6.6**. Организация реализует требования об ограничении доступа к информационным системам, в которых обрабатываются персональные данные.

**6.7**. Организация обеспечивает соблюдения режима обеспечения безопасности помещений, в которых обрабатываются в любом виде персональные данных. Указанный режим препятствует возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

**6.8**. Организация устанавливает и обеспечивает соблюдение требований к безопасности информационно-технических систем, применяемых при обработке персональных данных.

1. Договоры, указанные в настоящем пункте, не могут содержать положения, ограничивающие права и свободы Субъекта или устанавливающие случаи обработки персональных данных несовершеннолетних (если иное не предусмотрено законодательством России). Такие договоры также не могут содержать положения, допускающие в качестве условия заключения договора бездействие Субъекта. [↑](#footnote-ref-1)
2. Включая инструкции по заполнению, карточки, реестры, журналы и договоры, без ведения (заключения) которых невозможно заполнение типовой формы (либо заключение, ведение которых обусловлено заполнением типовой формы). [↑](#footnote-ref-2)