



Общество с ограниченной ответственностью
«Глобальные Брокерские Решения»

ПРИКАЗ

г. МОСКВА

«25» августа 2017 г.

№ 003-Д

Об введении в действие документов по обеспечению безопасности персональных данных в ООО «ГБС-Брокер»

В целях обеспечения безопасности персональных данных, а также в целях исполнения требований
Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных»

ПРИКАЗЫВАЮ:

1. Ввести в действие документы по обеспечению безопасности и персональных данных:
 - Положение о порядке обработки и защите персональных данных;
 - Политика в отношении обработки персональных данных;
 - Перечень персональных данных, обрабатываемых ООО «ГБС-Брокер».
2. Документы обязательны к исполнению во всех подразделениях Общества.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Приложение: Приложение №1 «Положение О порядке обработки персональных данных»;
Приложение №2 «Политика в отношении обработки персональных данных»;
Приложение №3 «Перечень персональных данных, обрабатываемых ООО
«ГБС-Брокер».

Генеральный директор

Степанов Р.В.



**Общество с ограниченной ответственностью
«Глобальные Брокерские Решения»**

Приложение № 1 к Приказу № 003 от 25 августа 2017

УТВЕРЖДАЮ

Генеральный директор
ООО «ГБС-Брокер»

«25»

августа

Р.В. Степанов
2017 г.

**Положение
о порядке обработки и защите персональных данных
в ООО "ГБС-Брокер".**

Введен в действие

«25»

августа

2017 г.

Приказ № 003 от «25» августа 2017 г.

Издание № 1

1. Общие положения

1.1. Назначение и область действия

- 1.1.1. Целью настоящего Положения является исполнение предусмотренных Законодательством РФ требований по обеспечению прав и свобод субъектов персональных данных при обработке их персональных данных в ООО «ГБС-Брокер», в том числе защита прав субъектов персональных данных на неприкосновенность частной жизни, личную и семейную тайну.
- 1.1.2. Настоящее Положение определяет цели обработки персональных данных, устанавливает общие требования к обеспечению безопасности персональных данных обрабатываемых ООО «ГБС-Брокер» (далее – Общество) с использованием средств автоматизации или без использования таких средств, основные задачи, функции и права подразделений, в обязанности которых входит проведение работ по организации защиты персональных данных.
- 1.1.3. Настоящее Положение разработано в соответствии с федеральным законодательством Российской Федерации.
- 1.1.4. Действие настоящего Положения распространяется на все структурные подразделения Общества.
- 1.1.5. Все работники Общества должны быть ознакомлены с настоящим Положением под роспись.
- 1.1.6. Настоящее Положение является локальным нормативным актом Общества и вступает в силу с момента подписания Генеральным директором приказа о введении его в действие.

1.2. Регламентирующие документы

- 1.2.1. Порядок обработки и обеспечения безопасности персональных данных, а также ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных регламентируют следующие нормативные правовые акты:
 - Гражданский кодекс Российской Федерации;
 - Уголовный кодекс Российской Федерации;
 - Кодекс Российской Федерации об административных правонарушениях;
 - Трудовой кодекс Российской Федерации;
 - Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных»;
 - Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 15.03.2013 г. № 274 "Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных"
 - Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
 - Постановление Правительства Российской Федерации от 15.09.2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
 - Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г.

№55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;

- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденному приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена заместителем директора ФСТЭК России 15.02.2008 г.;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена заместителем директора ФСТЭК России 14.02.2008 г.;
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 Центра ФСБ России 21.02. 2008 г. № 149/54 144.

1.2.2. Установление цели, условий получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а так же определение полномочий оператора, регламентируют следующие нормативные правовые акты:

- Федеральный закон «О связи» от 07.07.2003 г. № 126-ФЗ;
- Федеральный закон «Об акционерных обществах» от 26.12.1995 г. № 208-ФЗ;
- Федеральный закон «О государственной регистрации юридических лиц и индивидуальных предпринимателей» от 08.08.2001 г. № 129-ФЗ;
- Федеральный закон от 07.08.2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральный закон от 10.12.03 № 173-ФЗ «О валютном регулировании и валютном контроле»;
- Налоговый кодекс Российской Федерации 31.07.1998 г. № 146-ФЗ;

1.2.3. Организацию работы с информацией, относящейся к персональным данным, и материальными носителями, содержащими персональные данные, регламентируются нормативными и организационными документами Общества.

1.3. Список участвующих подразделений

Обработку персональных данных осуществляют все подразделения ООО «ГБС-Брокер» в части своей компетенции в соответствии с регламентами Общества.

2. Основные термины

2.1. В настоящем Положении используются следующие термины:

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Общество – ООО «ГБС-Брокер»;

биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Обществом для установления личности субъекта персональных данных;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

документ (официальный) – документ, созданный Обществом, а также юридическим или физическим лицом, оформленный (и/или удостоверенный) в установленном порядке;

доступ к информации, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну ООО «ГБС-Брокер», с согласия Общества или на ином законном основании при условии сохранения конфиденциальности этой информации;

информация, составляющая коммерческую тайну – имеющиеся у Общества сведения любого характера, которые обладают действительной или потенциальной коммерческой ценностью в силу их неизвестности третьим лицам, к которым нет свободного доступа на законном основании и в отношении которых Обществом введен режим коммерческой тайны;

коммерческая тайна – режим конфиденциальности информации, позволяющий Обществу при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

контрагент – сторона гражданско-правового договора с Обществом;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к информации, составляющей коммерческую тайну ООО «ГБС-Брокер», требование не передавать такую информацию третьим лицам без согласия Общества;

конфиденциальность персональных данных – обязательное для соблюдения оператором или иным, получившим доступ к персональным данным лицом, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

обладатель информации, составляющей коммерческую тайну – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

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;

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;

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

предоставление информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

разглашение информации, составляющей коммерческую тайну – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия Общества либо вопреки трудовому или гражданско-правовому договору;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

режим коммерческой тайны – правовые, организационные, технические и иные принимаемые Обществом в отношении информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности. Режим коммерческой тайны считается установленным после определения Перечня сведений, составляющих коммерческую тайну ООО «ГБС-Брокер»;

структурное подразделение Общества – структурное подразделение верхнего уровня (дирекция, департамент верхнего уровня, иное подразделение Общества), подчиняющееся Генеральному директору;

субъект персональных данных (Субъект ПДн) – физическое лицо, к которому относятся персональные данные;

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

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

3. Принципы и условия обработки персональных данных

3.1. Принципы обработки персональных данных в Обществе

3.1.1. При обработке персональных данных должны выполняться следующие принципы:

- Обработка персональных данных должна осуществляться на законной и справедливой основе.
- Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- Обработке подлежат только персональные данные, которые отвечают целям их обработки.
- 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.
- При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
- Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться 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. Обработываемые 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.

3.2. Способы обработки персональных данных

3.2.1. Общество может осуществлять обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

3.3. Конфиденциальность персональных данных

3.3.1. Работниками Общества, получившими доступ к персональным данным, обрабатываемым в Обществе, должна быть обеспечена конфиденциальность таких данных.

3.3.2. Обеспечение конфиденциальности не требуется в отношении:

- обезличенных персональных данных;
- персональных данных, сделанных общедоступными субъектом персональных данных;
- персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

3.3.3. Персональные данные отнесены Обществом к информации, составляющей коммерческую тайну, и включены в документально оформленный и утвержденный Приказом Генерального директора «Перечень сведений, составляющих коммерческую тайну ООО «ГБС-Брокер». Необходимый объем организационных мер, выполнение которых позволяет обеспечить конфиденциальность персональных данных в составе информации, составляющей коммерческую тайну, определен «Инструкцией по работе с документами, содержащими коммерческую тайну и сведения служебного характера ООО «ГБС-Брокер».

3.4. Передача персональных данных

3.4.1. Общество может поручить, с согласия субъекта персональных данных (если иное не предусмотрено федеральным законом), обработку персональных данных другому лицу на основании договора поручения.

3.4.2. Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом N 152-ФЗ «О персональных данных». В договоре поручения обработки персональных данных должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона N152-ФЗ «О персональных данных».

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

- 3.4.4. 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.

3.5. Общедоступные источники персональных данных

- 3.5.1. В целях информационного обеспечения в Обществе могут создаваться общедоступные источники персональных данных (телефонный справочник, адресная книга и т.п.).
- 3.5.2. В состав справочников могут входить фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом.
- 3.5.3. Обществом создаются общедоступные источники, содержащие персональные данные работников. Создание общедоступных источников персональных данных Обществом осуществляется на основе письменного согласия субъекта, чьи персональные данные включаются в создаваемые общедоступные источники. Согласие работника на создание общедоступных источников собирается в составе документа «Заявление работника о предоставлении согласия на обработку персональных данных», подписываемого каждым работником Общества.
- 3.5.4. Обществом раскрываются для неограниченного круга лиц в соответствии с федеральным законодательством с ведома и по письменному согласованию с субъектами персональных данных:
- сведения о работниках Общества, включаемые в Единый государственный реестр юридических лиц (ЕГРЮЛ) и являющиеся, в соответствии с Федеральным законом «О государственной регистрации юридических лиц и индивидуальных предпринимателей», открытыми и общедоступными;
 - сведения, относящиеся к персональным данным и подлежащие обязательному раскрытию и опубликованию в соответствии с федеральными законами «Об акционерных обществах»;
- 3.5.5. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.
- 3.5.6. Обязанность доказывания того, что персональные данные, обрабатываемые ООО «ГБС-Брокер» в общедоступных источниках персональных данных, включены в них с согласия субъекта персональных данных, возлагается на Общество.

3.6. Трансграничная передача персональных данных

- 3.6.1. Обществом осуществляется трансграничная передача персональных данных клиентов при осуществлении по поручению клиента операций с иностранными адресатами. При передаче персональных данных клиентов на территорию иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, Общество осуществляет такую трансграничную передачу персональных данных без запроса письменного согласия субъекта. При передаче персональных данных на территорию иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, Общество обязано 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. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных.

3.6.2. Трансграничная передача персональных данных клиентов на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться Обществом в случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- предусмотренных международными договорами Российской Федерации;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

3.7. Обработка персональных данных в целях продвижения продуктов и услуг на рынке

3.7.1. Обществом может производиться комплекс мероприятий по продвижению продуктов и услуг Общества путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, в рамках которого обрабатываются персональные данные клиентов только при условии их предварительного письменного согласия.

3.7.2. В случае отказа клиента от обработки его персональных данных в целях продвижения продуктов и услуг, Общество обязан немедленно прекратить обработку его персональных данных в указанных целях.

3.8. Принятие решений на основании исключительно автоматизированной обработки персональных данных

3.8.1. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Перед началом применения информационных систем для принятия на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении

субъекта персональных данных или иным образом затрагивающих его права и законные интересы, Общество обязано:

- разъяснить субъекту персональных данных порядок принятия и возможные юридические последствия такого решения,
- разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов,
- получить в письменной форме согласие субъекта персональных данных на такой способ принятия решений при обработке его персональных данных.

После принятия на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, Общество обязано:

- известить субъекта о принятом решении с целью предоставления возможности заявить возражение против такого решения,
- рассмотреть возражение, поступившее от субъекта персональных данных, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

3.8.2. В соответствии со ст. 86 Трудового кодекса, при принятии решений, затрагивающих интересы работников, Общество как работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Согласие субъекта персональных данных на обработку своих персональных данных

4.1. Обработка персональных данных в информационных системах Общества должна осуществляться только с согласия субъекта персональных данных, за исключением случаев, приведенных в п. 4.7 настоящего Положения.

4.2. Письменное согласие субъекта необходимо получать:

- на обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояние здоровья, интимной жизни, если только сам субъект не сделал эти сведения общедоступными;
- при обработке биометрических персональных данных;
- при включении персональных данных в общедоступные источники (справочники, адресные книги);
- в случаях трансграничной передачи персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных;
- при передаче обработки персональных данных другому лицу;
- при принятии на основании исключительно автоматизированной обработки персональных данных решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы.

4.3. Согласие субъекта персональных данных может быть получено как в отдельном документе, так и в составе документа, на котором субъект персональных данных проставляет личную подпись.

4.4. Документом, в составе которого может быть получено согласие субъекта персональных данных на обработку своих персональных данных, является:

- договор, заключаемый между субъектом персональных данных и Обществом, существенным условием которого является согласие субъекта на обработку Обществом его персональных данных;
 - платежное или иное поручение, передаваемое субъектом персональных данных Обществу в процессе получения услуги;
 - анкета, заполняемая субъектом персональных данных с целью получения услуги Общества или заключения договора с Обществом, одним из полей которой является отметка о согласии субъекта на обработку Обществом его персональных данных;
 - разовый пропуск субъекта персональных данных на территорию Общества, предусматривающий поле, в котором субъект персональных данных может проставить отметку о согласии субъекта на обработку Обществом его персональных данных;
 - иной документ, содержащий отметку о согласии субъекта на обработку его персональных данных Обществом, один из экземпляров которого передается Обществу (при наличии связанного текста согласия субъекта персональных данных на обработку его персональных данных, соответствующего требованиям ч.4 статьи 9 152-ФЗ).
- 4.5. Согласие субъекта персональных данных на обработку своих персональных данных в письменной форме должно включать в себя:
- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
 - фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
 - наименование и адрес Общества, как оператора, получающего согласие субъекта персональных данных;
 - цель обработки персональных данных;
 - перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
 - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка будет поручена такому лицу;
 - перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Обществом способов обработки персональных данных;
 - срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
 - подпись субъекта персональных данных.
- 4.6. Для обработки персональных данных, содержащихся в согласии, дополнительное согласие не требуется.
- 4.7. Согласие субъекта не требуется в случае, если:
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Общество функций, полномочий и обязанностей;
 - 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 защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
 - 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;
 - обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона «О персональных данных», при условии обязательного обезличивания персональных данных;
 - осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее — персональные данные, сделанные общедоступными субъектом персональных данных);
 - осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.
- 4.8. При запросе персональных данных, обработка которых не установлена требованиями законодательства или не требуется для исполнения договора, одной из сторон которого является субъект персональных данных, в дополнение к данным, полученным Обществом от субъекта в целях исполнения договора или требований законодательства, требуется получение согласия субъекта только на обработку дополнительно истребованных персональных данных Обществом.
- 4.9. Согласие на обработку персональных данных, обработка которых не установлена требованиями законодательства или не требуется для исполнения договора, одной из сторон которого является субъект персональных данных, может быть отозвано субъектом персональных данных. Действия работников Общества при отзыве согласия субъекта на обработку персональных данных установлены внутренним нормативным документом Общества «Регламент работы с обращениями субъектов персональных данных и запросами уполномоченного органа по защите прав субъектов персональных данных по вопросам, касающимся обработки персональных данных».
- 4.10. В случае возникновения необходимости предоставить доказательство получения согласия следует:
- в случае, если согласие входило в состав договора(анкеты), подписанного субъектом персональных данных предоставить заверенную копию договора(анкеты), вымарав на копии места, составляющие коммерческую тайну Общества (за исключением персональных данных субъекта)(при необходимости в исключительных случаях может быть представлен сам договор/анкета);
 - в случае, если согласие было получено отдельно, предоставить заверенную копию согласия субъекта персональных данных.

5. Категории персональных данных

5.1. В информационных системах Общества осуществляется обработка персональных данных относящихся ко второй, третьей и четвертой категориям из введенных в п.6 документа «Порядок проведения классификации информационных систем персональных данных» (утв. приказом ФСБ, ФСТЭК и Минкомсвязи России от 13.02.2008 г. №55/86/20:

- категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 - обезличенные и (или) общедоступные персональные данные.

Состав обрабатываемых персональных данных субъектов различных категорий, а также правовое основание, цели, сроки хранения и условия прекращения обработки, юридические последствия для субъекта персональных данных, вызванные такой обработкой, определены в «Перечне персональных данных ООО «ГБС-Брокер».

5.2. Специальные категории персональных данных

5.2.1. В Обществе не подлежат обработке персональные данные, относящиеся к специальным категориям:

- расовая принадлежность;
- национальная принадлежность;
- политические взгляды;
- религиозные или философские убеждения;
- состояния здоровья (за исключением состояния здоровья работников Общества в случаях, установленных ст. 69, 73, 213, 324, 328 Трудового кодекса РФ);
- интимная жизнь;
- персональные данные о частной жизни, о членстве субъектов персональных данных в общественных объединениях или их профсоюзной деятельности.

5.2.2. В случае принятия решения об обработке указанных категорий персональных данных, должно быть обеспечено выполнение одного из условий:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными.

5.2.3. Обработка персональных данных о судимости может осуществляться Обществом в случаях и порядке, которые определяются соответствующими федеральными законами.

6. Права субъектов персональных данных

6.1. В соответствии с действующим законодательством Российской Федерации Общество обязано обеспечить реализацию предусмотренных законодательством прав субъектов персональных данных. Субъект персональных данных вправе:

- получить сведения об Обществе как операторе персональных данных, о месте его нахождения, о наличии у Общества персональных данных, относящихся к этому субъекту персональных данных;
- ознакомиться со своими персональными данными, обрабатываемыми Обществом;

- обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
 - защищать свои права и законные интересы, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
- 6.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных. Обработка обращений субъектов персональных данных, направленных на осуществление прав субъектов персональных данных в соответствии со статьей 14 Федерального закона «О персональных данных» № 152-ФЗ от 27 июля 2006 г., осуществляется в соответствии с внутренним нормативным документом Общества «Правила взаимодействия с субъектами персональных данных в ООО «ГБС-Брокер».
- 6.3. Субъект персональных данных вправе требовать от Общества уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные 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.
- 6.4. Сведения о наличии персональных данных должны быть предоставлены представителем Общества субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.
- 6.5. Права субъекта персональных данных, предусмотренные Трудовым кодексом Российской Федерации, закрепляются во внутренних нормативных документах Общества, определяющих порядок обработки персональных данных работников ООО «ГБС-Брокер».

7. Хранение персональных данных

- 7.1.1. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных. Обработываемые персональные данные в соответствии с требованиями Федерального закона №152-ФЗ «О персональных данных» подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
- 7.1.2. Требования к хранению персональных данных, установленные Трудовым кодексом Российской Федерации, закреплены во внутреннем нормативном документе Общества «Положение о защите персональных данных работников».
- 7.1.3. При определении сроков хранения персональных данных, помимо целей обработки персональных данных, необходимо руководствоваться сроками исковой давности по гражданским делам (на основании Гражданского Кодекса), сроками хранения данных налогового учета (на основании налогового законодательства), установленными в Правилах внутреннего контроля в целях ПОД/ФТ сроками хранения со дня прекращения отношений с клиентом документов и сведений, представленных клиентом в результате проведения процедуры идентификации (на основании Федерального Закона от 07.08.2001 №115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"), приказом

Министра культуры Российской Федерации от 25.08.2010 г. N 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» и другими нормативными и законодательными актами Российской Федерации, устанавливающими сроки хранения (в том числе, архивного хранения) отдельных видов документов, содержащих персональные данные.

- 7.1.4. Обезличивание персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей применяется только в случае необходимости хранения персональных данных для обработки их в статистических или иных исследовательских целях (часть 9 статьи 6 Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных»). С учетом установленных в Правилах внутреннего контроля в целях ПОД/ФТ сроков хранения идентифицирующих данных клиентов, необходимость обезличивания ПДн в Обществе отсутствует.

8. Обязанности Общества при обработке персональных данных

8.1. Обязанности Общества при сборе персональных данных

- 8.1.1. Если обязанность предоставления персональных данных субъектом установлена федеральным законом, представитель Общества обязан разъяснить субъекту персональных данных юридические последствия отказа в предоставлении своих персональных данных.
- 8.1.2. Такими последствиями отказа в предоставлении своих персональных данных могут быть:
- для работника – отказ в заключении трудового договора с работодателем (для соискателей должностей), невозможность предоставления социальных льгот и дополнительных мер социальной защиты;
 - для клиента – отказ в предоставлении (заказе) услуг.
- 8.1.3. Если персональные данные были получены Обществом не от субъекта персональных данных, а от другого лица или другого оператора персональных данных, за исключением случаев, когда:
- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
 - персональные данные получены Обществом на основании федерального закона или в связи с исполнением договора, стороной которого является субъект персональных данных;
 - персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
 - Общество осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;
 - предоставление субъекту персональных данных сведений нарушает права и законные интересы третьих лиц,
- то до начала обработки таких персональных данных Общество обязано предоставить субъекту персональных данных следующую информацию:
- наименование и адрес Общества или его представителя;
 - цель обработки персональных данных и ее правовое основание;
 - предполагаемые пользователи персональных данных;
 - установленные законом права субъекта персональных данных;
 - источник получения персональных данных.

8.1.4. Обязанности Общества при сборе персональных данных, установленные Трудовым кодексом Российской Федерации, закреплены во внутреннем нормативном документе Общества «Положение об обработке персональных данных работников ООО «ГБС-Брокер».

8.2. Организация обработки персональных данных

8.2.1. В соответствии с требованиями Федерального закона N 152-ФЗ «О персональных данных» в Обществе назначается лицо, ответственное за организацию обработки персональных данных.

8.2.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от Генерального директора Общества и подотчетно ему.

8.2.3. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

- осуществлять внутренний контроль за соблюдением Обществом и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Общества положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку Обществом обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

8.2.4. Руководители структурных подразделений верхнего уровня, территориальных управлений и филиалов Общества обязаны оперативно предоставлять необходимые материалы и сведения по запросам лица, ответственного за организацию обработки персональных данных в Обществе, а также устранять нарушения требований законодательства Российской Федерации при работе с персональными данными, в случае выявления их в подразделении.

8.2.5. Общество обеспечивает публикацию в информационно-телекоммуникационной сети общего доступа документа, определяющего его политику в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных. Таким документом является Политика в отношении обработки персональных данных ООО «ГБС-Брокер».

8.3. Меры по обеспечению безопасности персональных данных при их обработке

8.3.1. Общество при обработке персональных данных принимает необходимые правовые, организационные и технические меры 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.

8.3.2. 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;
- 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;
- осуществлять контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;
- обеспечить доведение до сведения работников Общества положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и контролировать эти процессы.

8.3.3. Общество предоставляет лицу, ответственному за организацию обработки персональных данных сведения об обработке персональных данных, в соответствии с требованиями действующего законодательства в области персональных данных.

8.3.4. Общество разрабатывает должностную инструкцию ответственного за организацию обработки персональных данных.

8.3.5. В составе информационных систем персональных данных Общества должна применяться подсистема, обеспечивающая защиту 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.

- 8.3.6. Система защиты персональных данных реализуется организационными и техническими мерами и применением средств защиты информации.
- 8.3.7. Распределение ответственности между подразделениями Общества, содержание и периодичность выполнения организационно-технических мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Общества регламентируется нормативным документом.
- 8.4. Финансирование мероприятий по обеспечению безопасности персональных данных
 - 8.4.1. Финансирование мероприятий по обеспечению безопасности персональных данных осуществляется за счет средств ООО «ГБС-Брокер» и предусматривается соответствующим пунктом бюджета.
- 8.5. Ответственность за нарушение требований законодательства
 - 8.5.1. Лица, виновные в нарушении требований действующего федерального законодательства Российской Федерации в области персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность.

9. Мероприятия по обеспечению безопасности персональных данных

9.1. Общие положения

- 9.1.1. Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Общества.
- 9.1.2. Организация работ по обеспечению безопасности персональных данных осуществляется руководством Общества.
- 9.1.3. Ответственность за разработку и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Общества, распределяется между уполномоченными на выполнение данных работ подразделениями Общества приказом Генерального директора. Приказом Генерального директора на руководителей структурных подразделений верхнего уровня, территориальных управлений и филиалов Общества возлагается ответственность за обеспечение соблюдения требований законодательства Российской Федерации в области обработки персональных данных и требований внутренних нормативных документов Общества при организации работ, включающих обработку персональных данных, в возглавляемых ими подразделениях.
- 9.1.4. Для выбора и реализации методов и способов защиты информации Обществом должны привлекаться организации, имеющие оформленные в установленном порядке лицензии на осуществление деятельности по технической защите конфиденциальной информации и/или на осуществление деятельности в области шифрования информации.

- 9.2. Обеспечение безопасности персональных данных при автоматизированной обработке
- 9.2.1. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.
- 9.2.2. Безопасность персональных данных при их обработке в информационной системе персональных данных (ИСПДн) обеспечивается системой защиты персональных данных, включающей организационные и технические меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Состав средств защиты информации определяется в документе «Модель угроз», формируемом для каждой информационной системы персональных данных Общества, и может включать в себя шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных.
- 9.2.3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах Общества являются неотъемлемой частью работ по созданию и вводу в эксплуатацию информационных систем.
- 9.2.4. Права и обязанности подразделений и лиц, ответственных за безопасность персональных данных при обработке их в ИСПДн, устанавливаются «Политикой информационной безопасности ООО «ГБС-Брокер» и другими внутренними регламентирующими документами Общества.
- 9.2.5. Для определения угроз безопасности персональных данных при их обработке в Обществе должен быть разработан документ «Информационная система персональных данных ООО «ГБС-Брокер». Модель актуальных угроз безопасности. Модель нарушителя».
- 9.2.6. На основе модели угроз разрабатывается система защиты персональных данных, обеспечивающая нейтрализацию предполагаемых угроз. Для технического проектирования и реализации в Обществе системы защиты персональных данных может привлекаться только специализированная организация, имеющая необходимый набор лицензий в области технической защиты конфиденциальной информации. Комплект проектной документации на систему защиты персональных данных должен в обязательном порядке входить в состав эксплуатационной документации системы защиты персональных данных Общества. Эксплуатационная документация системы защиты персональных данных должна также включать описание системы защиты ИСПДн.
- 9.2.7. Должна производиться проверка готовности средств защиты информации к использованию. Готовность средств защиты информации к использованию в составе информационной системы персональных данных Общества закрепляется заключениями о возможности эксплуатации средств защиты.
- 8.4.1 В соответствии с разработанной документацией в Обществе производится установка и ввод в эксплуатацию средств защиты информации. Учет применяемых средств защиты информации производится в соответствии с их эксплуатационной документацией.
- 9.2.8. Лица, доступ которых к персональным данным, обрабатываемым в Обществе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к обработке персональных данных на основании «Регламента предоставления допуска к обработке персональных данных». Разрешение на

допуск включает Обязательство по обеспечению конфиденциальности и безопасности персональных данных. Данный порядок предоставления доступа к персональным данным регламентируется приказом Генерального директора.

9.2.9. Обязанности лиц, допускаемых к работе с персональными данными, определяются соответствующим разделом должностных инструкций.

9.3. Классификация информационных систем персональных данных

Все информационные системы персональных данных (далее – ИСПДн) Общества классифицируются комиссией, назначенной приказом Генерального директора Общества. Классификация осуществляется в соответствии с порядком, определенным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. N 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных». Результаты классификации оформляются актом, утверждаемым Генеральным директором Общества.

8.5 Система защиты персональных данных

8.4.1 Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные и технические меры и средства защиты информации. Выбор и реализация методов и способов защиты ПДн в информационной системе осуществляется на основе класса ИСПДн и исходя из угроз безопасности персональных данных, определенных в модели угроз, разрабатываемой в соответствии с методическими документами Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

8.4.2 При обработке персональных данных в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

8.4.3 Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя организационно-технические меры:

- назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- ограничение и регламентация состава работников, имеющих доступ к персональным данным;
- ознакомление работников с требованиями федерального законодательства и нормативных документов Общества по обработке и защите персональных данных;

- обеспечение учёта и хранения материальных носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение;
- определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
- разработку на основе модели угроз системы защиты персональных данных для соответствующего класса информационных систем;
- проверку готовности и эффективности использования средств защиты информации;
- реализацию разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- регистрацию и учёт действий пользователей информационных систем персональных данных;
- парольную защиту доступа пользователей к информационной системе персональных данных;
- применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;
- применение межсетевого экранирования;
- обнаружение вторжений в корпоративную сеть Общества, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищённости информационных систем персональных данных Общества с применением специализированных программных средств (сканеров безопасности);
- централизованное управление системой защиты персональных данных.
- резервное копирование информации;
- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;
- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- систематическое проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;
- размещение технических средств обработки персональных данных, в пределах охраняемой территории;
- организацию пропускного режима на территорию Общества, охраны помещений и собственно технических средств обработки персональных данных;

- поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности, ведение видеонаблюдения.
- 8.4.4 Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
- 8.5 Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации
 - 8.5.1 Обработка персональных данных без использования средств автоматизации осуществляется в режиме коммерческой тайны в соответствии с «Инструкцией по работе с документами, содержащими коммерческую тайну и сведения служебного характера ООО «ГБС-Брокер».
 - 8.5.2 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).
 - 8.5.3 При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
 - 8.5.4 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
 - 8.5.5 Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы:
 - о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации;
 - о категориях обрабатываемых персональных данных;
 - об особенностях и правилах осуществления такой обработки.
 - 8.5.6 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:
 - типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Общества, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Обществом способов обработки персональных данных;
 - при необходимости получения письменного согласия на обработку персональных данных типовая форма должна предусматривать поле, в котором

субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8.5.7 Подготовка документов, содержащих персональные данные, осуществляется работниками, имеющими допуск к обработке персональных данных. При подготовке документов соблюдаются требования фирменного стиля Общества с использованием фирменных бланков и фирменных шрифтов.

8.5.8 Печать документов, содержащих персональные данные, производится исполнителями документов. При подготовке документов с помощью стандартных сетевых рабочих станций соблюдаются требования обеспечения безопасности информации при работе в автоматизированных системах ООО «ГБС-Брокер», правил оформления документов, создаваемых в ООО «ГБС-Брокер» и требования комплекса документов по обработке и обеспечению безопасности персональных данных в ООО «ГБС-Брокер», в том числе настоящего Положения.

8.5.9 На оборотной стороне последнего листа визового экземпляра документа, предназначенного для помещения в дело, лицо, ответственное за работу с документами, содержащими персональные данные, или исполнитель проставляет отметку, включающую в себя количество отпечатанных экземпляров, дату документа, сведения о направлении каждого экземпляра, фамилию исполнителя.

8.5.10 Если документ дополнительно размножался, проставляется отметка о количестве размноженных экземпляров с указанием их номеров. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

8.5.11 Дела с документами, содержащими персональные данные, должны иметь внутренние описи. Внутренняя опись дела нумеруется отдельно.

8.5.12 Карточки регистрации документов помещаются в картотеки структурных подразделений или лица, ответственного за работу с документами с грифом «Коммерческая тайна», и используются для контроля за наличием документа, его прохождением, размножением, а также для внесения информации о помещении документа в дело или уничтожении. Срок хранения картотеки на документы, содержащие персональные данные/традиционных регистрационных форм на бумажных носителях (при их наличии) определяется номенклатурой дел филиала/ Сводной номенклатурой дел Общества.

8.5.13 Завершенные дела, содержащие персональные данные, постоянного и временного (более пяти лет) хранения передаются на архивное хранение.

8.5.14 Размножение документов содержащих персональные данные осуществляется работниками, ответственными за работу с документами содержащими персональные данные.

Размножение документов с персональными данными допускается только с разрешения руководителя структурного подразделения или филиала с

обязательной отметкой о размножении в карточках регистрации документов и на самих документах.

8.5.15 Входные двери помещений, где хранятся документы содержащие персональные данные, должны быть оборудованы замками, гарантирующими надежное закрытие помещения в нерабочее время.

Для контроля за входом могут устанавливаться кодовые замки или иные средства защиты, в необходимых случаях помещения оснащаются охранной сигнализацией.

Документы содержащие персональные данные хранятся в сейфах или металлических шкафах.

8.5.16 После окончания рабочего дня сейфы, металлические шкафы и двери помещений, не оборудованные кодовыми замками, запираются.

- О фактах утраты ключа от сейфа, металлического шкафа или входной двери помещения, где хранятся документы, содержащие персональные данные, сообщается в Службу безопасности и руководителю филиала/руководителю структурного подразделения. Замок этого помещения или двери помещения должны быть заменены или изменен секрет замка.

- Хранение документов, содержащих персональные данные в сейфах, помещениях, от которых утрачены ключи, до замены замка или изменения его секрета запрещается.

- Сейфы, металлические шкафы, помещения, в которых хранятся документы содержащие персональные данные, могут быть вскрыты комиссией, созданной по указанию директора филиала, о чем составляется акт.

8.5.17 О фактах утраты документов, содержащих персональные данные или разглашения содержащихся в них сведений немедленно ставится в известность директор филиала и/или руководитель структурного подразделения, Директор Службы безопасности и руководитель Общества, ответственный за обработку персональных данных. На утраченные документы, содержащие персональные данные, составляется акт. Соответствующие отметки вносятся в карточки регистрации документов/традиционные регистрационные формы.

8.5.18 Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

8.5.19 Порядок уничтожения персональных данных регламентирован документом ООО «ГБС-Брокер».

9. Подразделения, осуществляющие функции по организации защиты персональных данных

9.1. Общие положения

9.1.1 Основной задачей подразделений Общества при осуществлении функции по защите персональных данных является обеспечение безопасности персональных данных при их обработке в Обществе путем предотвращения утечки персональных данных по техническим каналам, исключения несанкционированного доступа к ним, предупреждения преднамеренных программно-технических воздействий, предпринимаемых с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения.

9.1.2 В своей деятельности по защите персональных данных Общество руководствуется законодательными и нормативно-правовыми актами

Российской Федерации, настоящим Положением и иными нормативными актами Общества.

- 9.1.3 Подразделения в части выполнения функций организации защиты персональных данных подчиняются Генеральному директору Общества.
 - 9.1.4 Персональную ответственность за выполнение закрепленных за подразделением мероприятий по обеспечению безопасности персональных данных несут руководители подразделений, осуществляющих функции по организации защиты персональных данных.
- 9.2 Обязанности, права и ответственность лиц, ответственных за обеспечение безопасности персональных данных
- 9.2.1 Лицами, ответственными за обеспечение безопасности персональных данных, являются руководители подразделений, уполномоченных на проведение работ по разработке и осуществлению мероприятий по обеспечению защиты персональных данных при их обработке в информационных системах Общества.
 - 9.2.2 Лица, ответственные за обеспечение безопасности персональных данных, обязаны осуществлять функции контроля деятельности подчиненного подразделения, осуществляющего мероприятия по обеспечению безопасности персональных данных.
 - 9.2.3 Лица, ответственные за обеспечение безопасности персональных данных, руководствуются в своей практической деятельности положениями нормативно-правовых актов Российской Федерации и внутренними распорядительными документами Общества.
 - 9.2.4 Требования лиц, ответственных за обеспечение безопасности персональных данных, связанные с выполнением возложенных на них функций, обязательны для исполнения всеми пользователями ИСПДн.

9.2.5 Лица, ответственные за обеспечение безопасности персональных данных, отвечают за организацию:

- проведения мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременного обнаружения фактов несанкционированного доступа к персональным данным;
- недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- возможности незамедлительного восстановления персональных данных,
- модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянного контроля за обеспечением уровня защищенности ПДн.

9.2.6 Лица, ответственные за обеспечение безопасности персональных данных несут персональную ответственность за качество проводимых ими работ по организации обеспечения защиты персональных данных.

9.3 Функции службы безопасности Общества

- Организация обучения лиц, применяющих средства защиты информации, правилам работы с ними.
- Организация и контроль работ по обеспечению безопасности обработки персональных данных в информационных системах персональных данных.
- Организация приема и обработки Обществом обращений и запросов субъектов персональных данных или их представителей.

9.4 Функции информационно технических служб Общества

- Организация учета и использования магнитных, оптических и других машинных носителей информации, предназначенных для обработки персональных данных.
- Учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных (предоставление на основе заявок прав доступа пользователей к информационным системам персональных данных, учет таких заявок и предоставленных пользователям прав).
- Организация мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

9.5 Функции служб по работе с персоналом Общества

Анализ и оценка соответствия внутренних нормативных документов Общества, в части касающейся обработки персональных данных работников Общества, требованиям законодательства Российской Федерации в области персональных данных, а в случае выявления несоответствий – внесение необходимых изменений, в том числе в должностные инструкции персонала.

9.6 Функции юридической службы Общества

- Анализ законодательства Российской Федерации в области персональных данных.
- Согласование направляемого в уполномоченный орган по защите прав субъектов персональных данных Уведомления об обработке персональных данных, а в случае изменения сведений, содержащихся в Реестре операторов осуществляющих обработку персональных данных – согласование направляемых сведений о таких изменениях.

- Анализ и оценка соответствия типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства Российской Федерации в области персональных данных, а в случае выявления несоответствий - выработка рекомендаций по их устранению.
- Анализ и оценка соответствия договорной базы Общества требованиям законодательства Российской Федерации в области персональных данных, а в случае выявления несоответствий – внесение соответствующих изменений (дополнений).

9.7 Функции подразделений, обрабатывающих персональные данные

- выполнение работ по обращениям субъектов персональных данных, в том числе:
 - ✓ оформление обращений субъектов персональных данных и их представителей в офисах Общества;
 - ✓ внесение уточнений в персональные данные субъектов;
 - ✓ реализация решения о блокировании обработки персональных данных субъектов;
 - ✓ принятие и реализация решения об уничтожении персональных данных (по достижении целей обработки или в случае утраты необходимости в их достижении) при их автоматизированной обработке;
 - ✓ подготовка материалов для уведомления субъектов в установленных законодательством случаях (об обработке персональных данных, о внесении изменений в персональные данные, о прекращении обработки и уничтожении персональных данных, об отказе в предоставлении субъекту сведений).
- подготовка материалов для уведомления субъектов персональных данных об устранении нарушений, связанных с неправомерными действиями в отношении их персональных данных, в случае обращения или запроса субъекта персональных данных; в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, уведомление уполномоченного органа.

9.8 Подразделения, осуществляющие функции по организации защиты персональных данных имеют право в пределах их компетенции на:

- Запрос и получение необходимых материалов для организации и проведения работ по вопросам обеспечения безопасности персональных данных в Обществе.
- Привлечение к проведению работ по защите персональных данных других подразделений Общества.
- Привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций.
- Контроль деятельности структурных подразделений Общества в части выполнения ими требований по обеспечению безопасности персональных данных.
- Внесение предложений Генеральному директору Общества о приостановке обработки персональных данных в случае обнаружения несанкционированного доступа, утечки персональных данных, а также в случае предпосылок нарушения безопасности персональных данных.

10. Контроль выполнения требований настоящего Положения

- 10.1. Перечень мероприятий по контролю, его периодичность, а также ответственные лица устанавливаются внутренним документом Общества.
- 10.2. В ходе внутренних проверок осуществляются мероприятия, определенные действующим законодательством Российской Федерации в области персональных данных, а также требования, предъявляемые к системе защиты ПДн информационных систем персональных данных Общества.

11. Ответственность за нарушение требований настоящего Положения

- 11.1. Нарушение настоящего Положения может повлечь за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.
- 11.2. Работник Общества, который в связи с исполнением трудовых обязанностей получил доступ к персональным данным, в случае умышленного или неосторожного разглашения этой информации, при отсутствии в действиях такого работника состава преступления, несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.
- 11.3. Юридическое лицо, не выполнившее установленные законом обязанности по обеспечению конфиденциальности и безопасности персональных данных, несет ответственность в соответствии с законодательством Российской Федерации

Дополнительные должностные обязанности работников в связи с обработкой персональных данных

Наименование раздела должностной инструкции	Формулировка
<i>Предназначение</i>	Соблюдение требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».
<i>Основные функции</i>	Соблюдение требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», в т.ч.: • соблюдает принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных»; • обеспечивает в соответствии с требованиями действующего законодательства РФ и внутренних нормативных документов Общества конфиденциальность персональных данных и безопасность персональных данных, ставших ему доступными в связи с исполнением должностных обязанностей.
<i>Ответственность</i>	Несоблюдение требований Федерального закона 27.07.2006 №152-ФЗ «О персональных данных», в т.ч. ¹ : • разглашение персональных данных работников Общества, клиентов Общества и иных лиц (далее – персональные данные), которые станут ему известны при выполнении им своих должностных обязанностей; • распространение (устно/письменно) персональных данных без соответствующего письменного указания уполномоченного на то должностного лица Общества; • несвоевременное (позже даты выявления) извещение (устно/письменно/любыми доступными средствами связи) непосредственного руководителя и Службы безопасности о выявленных фактах/попытках незаконного получения третьими лицами персональных данных; • несвоевременную (позже последнего дня работы в занимаемой должности) передачу непосредственному руководителю/работнику, которому руководителем предоставлен доступ к персональным данным, в соответствии с установленным в Обществе порядком, всех носителей персональных данных (личные дела, трудовые книжки, другие документы, содержащие персональные данные, машинные носители информации, черновики и пр.), которые находились в его распоряжении, при переводе на другую должность/увольнении; • несвоевременное (позже даты выявления) извещение (устно/письменно/любыми доступными средствами связи) Службы безопасности о выявленных им фактах утраты/недостачи любых носителей информации, содержащих персональные данные, пропусков, ключей от сейфов (хранилищ), личных печатей, иных фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях возможной утечки этих сведений.

¹ В случае, если руководителем подразделения работник включен в список работников подразделения, которым в соответствии со служебными (трудовыми) обязанностями предоставляется доступ к персональным данным, обрабатываемым в ООО «ГБС-Брокер» с использованием средств автоматизации или без использования таких средств