

**Положение об обработке и защите  
персональных данных  
ООО «Ренессанс Брокер»**

## Оглавление

<b>СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ .....</b>	<b>4</b>
<b>1. ОБЩИЕ ПОЛОЖЕНИЯ .....</b>	<b>5</b>
<b>2. ЛИЦА, ПРИНИМАЮЩИЕ УЧАСТИЕ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>5</b>
<b>3. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ .....</b>	<b>8</b>
<b>3.1. ОБЩЕЕ ОПИСАНИЕ МЕР .....</b>	<b>8</b>
<b>3.2. ПОРЯДОК ОПРЕДЕЛЕНИЯ ПЕРЕЧНЯ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>9</b>
<b>3.3. ПОРЯДОК ОПРЕДЕЛЕНИЯ ПЕРЕЧНЯ ДОЛЖНОСТЕЙ РАБОТНИКОВ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>10</b>
<b>3.4. ПОРЯДОК ПОЛУЧЕНИЯ СОГЛАСИЯ СУБЪЕКТОВ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>11</b>
<b>4. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>13</b>
<b>4.1. ПРИНЦИПЫ И ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>13</b>
<b>4.2. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКАМ КОМПАНИИ .....</b>	<b>13</b>
<b>4.3. ПОРЯДОК СБОРА И УТОЧНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>14</b>
<b>4.4. ПОРЯДОК ПЕРЕДАЧИ И ПРЕДОСТАВЛЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМИ ЛИЦАМИ .....</b>	<b>15</b>
<b>4.5. ПОРЯДОК ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>15</b>
<b>4.6. ПОРЯДОК ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>16</b>
<b>4.7. ПОРЯДОК ХРАНЕНИЯ И УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>16</b>
<b>4.8. ПОРЯДОК БЛОКИРОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>17</b>
<b>4.9. ПОРЯДОК ОБРАЩЕНИЯ С МАТЕРИАЛЬНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>17</b>
<b>4.10. ПОРЯДОК НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>18</b>
<b>5. ПРАВА И ОБЯЗАННОСТИ СТОРОН .....</b>	<b>19</b>
<b>5.1. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ .....</b>	<b>19</b>
<b>5.2. ПРАВА И ОБЯЗАННОСТИ КОМПАНИИ КАК ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ</b>	<b>22</b>
<b>5.3. ОБЯЗАННОСТИ РАБОТНИКОВ КОМПАНИИ В ЧАСТИ ЗАЩИТЫ И ХРАНЕНИЯ ПДН</b>	<b>24</b>
<b>6. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ И УПОЛНОМОЧЕННЫМ ОРГАНОМ ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ .....</b>	<b>25</b>
<b>6.1. ОБЩИЕ ПРАВИЛА ВЗАИМОДЕЙСТВИЯ С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>	<b>25</b>

<b>6.2. ПОРЯДОК РЕАГИРОВАНИЯ НА ЗАПРОСЫ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>	
25	
<b>6.3. ОБЩИЕ СВЕДЕНИЯ О ДЕЯТЕЛЬНОСТИ УПОЛНОМОЧЕННОГО ОРГАНА В РАМКАХ ГОСУДАРСТВЕННОГО КОНТРОЛЯ И НАДЗОРА.....</b>	<b>27</b>
<b>6.4. ПОРЯДОК ДЕЙСТВИЙ В РАМКАХ ПРОВЕРОК УПОЛНОМОЧЕННОГО ОРГАНА.....</b>	<b>28</b>
<b>7. КОНТРОЛЬ ПРИНИМАЕМЫХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>31</b>
<b>7.1. ОБЩИЕ ПОЛОЖЕНИЯ О ПОРЯДКЕ ПРОВЕДЕНИЯ МЕРОПРИЯТИЙ ПО МОНИТОРИНГУ И КОНТРОЛЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>31</b>
<b>7.2. ПОРЯДОК ПРОВЕДЕНИЯ ПЕРИОДИЧЕСКИХ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ.....</b>	<b>32</b>
<b>7.3. ПОРЯДОК ПРОВЕДЕНИЯ СЛУЖЕБНЫХ РАССЛЕДОВАНИЙ.....</b>	<b>33</b>
<b>7.4. ПОРЯДОК ПРОВЕДЕНИЯ ВНЕШНИХ АУДИТОВ.....</b>	<b>34</b>
<b>8. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ НЕШТАТНЫХ СИТУАЦИЙ.....</b>	<b>35</b>
<b>9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ПОЛОЖЕНИЯ.....</b>	<b>36</b>
<b>10. ПОРЯДОК ПЕРЕСМОТРА ПОЛОЖЕНИЯ.....</b>	<b>36</b>
<b>ПРИЛОЖЕНИЕ 1. ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>37</b>
<b>ПРИЛОЖЕНИЕ 2. ФОРМА ПЕРЕЧНЯ ХРАНИЛИЩ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>39</b>
<b>ПРИЛОЖЕНИЕ 3. ФОРМА ЖУРНАЛА УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>40</b>
<b>ПРИЛОЖЕНИЕ 4. АКТ О ВЫДЕЛЕНИИ К УНИЧТОЖЕНИЮ И УНИЧТОЖЕНИИ БУМАЖНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, НЕ ПОДЛЕЖАЩИХ ХРАНЕНИЮ.....</b>	<b>41</b>
<b>ПРИЛОЖЕНИЕ 5. ФОРМА ЗАПРОСА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>43</b>
<b>ПРИЛОЖЕНИЕ 6. ФОРМА ЖУРНАЛА УЧЕТА ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И УПОЛНОМОЧЕННОГО ОРГАНА ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>44</b>
<b>ПРИЛОЖЕНИЕ 7. ТИПОВАЯ ФОРМА ОТВЕТА НА ЗАПРОС СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>45</b>
<b>ПРИЛОЖЕНИЕ 8. ТИПОВАЯ ФОРМА ЖУРНАЛА УЧЕТА ПРОВЕРОК КОМПАНИИ, ПРОВОДИМЫХ ОРГАНАМИ ГОСУДАРСТВЕННОГО КОНТРОЛЯ (НАДЗОРА), ОРГАНАМИ МУНИЦИПАЛЬНОГО КОНТРОЛЯ.....</b>	<b>47</b>

## Список терминов и сокращений

ПДн	–	персональные данные
ИСПДн	–	информационная система персональных данных
Роскомнадзор	–	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
ФЗ	–	Федеральный закон
ФИО	–	фамилия, имя, отчество

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

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

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

**Автоматизированная обработка ПДн** – обработка ПДн с помощью средств вычислительной техники.

**Распространение ПДн** – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

**Предоставление ПДн** – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

**Блокирование ПДн** – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

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

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

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

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

## 1. Общие положения

1.1. Положение о ПДн ООО «Ренессанс Брокер» (далее – Положение) определяет требования к порядку обработки и обеспечению безопасности ПДн при их обработке с использованием средств автоматизации и без использования таких средств в ООО «Ренессанс Брокер» (далее – Компания).

1.2. Положение разработано в соответствии с требованиями следующих правовых актов:

- Конституции Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Трудового кодекса Российской Федерации;
- Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Требования настоящего Положения обязательны для выполнения работниками Компании, которые в силу должностных обязанностей имеют доступ к ПДн, обрабатываемым в Компании.

1.4. По предмету регулирования настоящее Положение охватывает все аспекты деятельности Компании, касающиеся обращения ПДн субъектов, а также передачу ПДн третьим лицам.

1.5. Настоящее Положение утверждается и вводится в действие приказом Генерального директора Компании.

## 2. Лица, принимающие участие в обеспечении безопасности персональных данных

2.1. В целях организации и проведения работ по обеспечению безопасности ПДн в Компании определяются роли и назначаются ответственные лица и подразделения:

- лицо, ответственное за организацию обработки ПДн – определяется отдельным приказом Компании;
- подразделение, ответственное за реализацию мероприятий по защите ПДн – Департамент информационных технологий либо иное подразделение, определенное специальным приказом Компании;
- подразделение, ответственное за юридическое обеспечение деятельности по защите ПДн – Юридическое управление;
- подразделение, ответственное за прием и отправку почтовой корреспонденции – Управление корпоративной поддержки либо иное подразделение, определенное специальным приказом Компании;
- лица, ответственные за исполнение работниками структурных подразделений Компании требований к защите ПДн – руководители структурных подразделений Компании.

2.2. Лицо, ответственное за организацию обработки ПДн, получает указания непосредственно от Генерального директора Компании, и подотчетно ему.

2.3. Лицо, ответственное за организацию обработки ПДн, обязано:

- доводить до сведения работников Компании положения законодательства Российской Федерации о ПДн, локальных актов Компании по вопросам обработки ПДн, требований к защите ПДн;
- разрабатывать локальные акты по вопросам обработки ПДн, предотвращения и выявления нарушений требований к защите ПДн;
- оценивать вред, который может быть причинен субъектам ПДн в случае нарушения требований к защите ПДн, соотношение указанного вреда и принимаемых Компанией мер по обеспечению безопасности ПДн;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов;
- регистрировать запросы субъектов ПДн и ответов на такие запросы;
- осуществлять внутренний контроль соблюдения Компанией и ее работниками законодательства Российской Федерации о ПДн и локальных актов Компании по вопросам обработки ПДн;
- инициировать расследование инцидентов нарушения безопасности ПДн и устранение последствий таких нарушений;
- регистрировать уведомления о проверках регулирующих организаций, а также ответов на запросы регулирующих организаций;
- сопровождать проверки соблюдения требований к защите ПДн, инициируемые регулируемыми организациями.

2.4. Подразделение, ответственное за реализацию мероприятий по защите ПДн, обязано:

- проектировать систему защиты ПДн, включающую физические и технические меры и средства защиты;
- закупать, устанавливать и настраивать технические средства защиты информации;
- проводить работы по учету, хранению и уничтожению машинных носителей ПДн;
- осуществлять изменение, уничтожение, удаление, блокирование ПДн, обрабатываемых в ИСПДн по запросам субъектов ПДн и уполномоченного органа по защите прав субъектов ПДн;
- инструктировать и обучать работников, которые в силу своих служебных обязанностей имеют доступ к ПДн, использованию технических средств защиты информации;
- принимать участие в расследованиях инцидентов нарушения безопасности ПДн и проверках, инициируемых регулируемыми организациями.

2.5. Подразделение, ответственное за юридическое обеспечение деятельности по защите ПДн, обязано:

- предоставлять консультации лицу, ответственному за организацию обработки ПДн, в части юридических аспектов обработки ПДн;
- проводить юридическую оценку правомерности запросов субъектов ПДн об обработке их ПДн;

- проводить юридическую оценку правомерности запросов государственных, муниципальных органов на предоставление сведений, включающих обрабатываемые в Компании ПДн;
- составлять мотивированные отказы в предоставлении сведений, включающих ПДн, по запросам субъектов ПДн и государственных, муниципальных органов;
- обеспечивать заключение с третьими лицами договоров, соответствующих требованиям к защите ПДн, если предметом договора является поручение на обработку ПДн;
- выполнять юридическое сопровождение проверок, инициируемых регулирующими организациями.

2.6. Подразделение, ответственное за прием и отправку почтовой корреспонденции, обязано:

- осуществлять прием письменных запросов субъектов ПДн, государственных, муниципальных органов на предоставление сведений, включающих обрабатываемые в Компании ПДн и отправку ответов на такие запросы;
- осуществлять прием уведомлений о проверках регулирующих организаций, а также отправку ответов на запросы регулирующих организаций.

2.7. Лица, ответственные за исполнение работниками структурных подразделений Компании требований к защите ПДн, обязаны:

- доводить до сведения работников структурных подразделений Компании требования к защите ПДн;
- контролировать выполнение требований локальных актов Компании по вопросам обработки ПДн, работниками структурных подразделений;
- назначать исполнителей для подготовки ответов на запросы о предоставлении сведений, включающих ПДн, от субъектов ПДн, государственных и муниципальных органов;
- ставить в известность лицо, ответственное за организацию обработки ПДн, о фактах нарушения правил обработки ПДн работниками структурного подразделения и иных фактах, которые могут привести к нарушению целостности, доступности и конфиденциальности ПДн, обрабатываемых в Компании.

2.8. Лица, принимающие участие в обеспечении безопасности ПДн, имеют право:

- запрашивать у работников Компании и знакомиться с документами и материалами, необходимыми для выполнения возложенных задач;
- привлекать в установленном порядке специалистов, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе внутреннего контроля выполнения требований по защите ПДн или расследования нарушения безопасности ПДн, и выработки обоснованных рекомендаций и заключений;
- вносить руководителям структурных подразделений Компании предложения о приостановлении действий, противоречащих законодательству Российской Федерации о ПДн и локальным актам Компании по вопросам обработки ПДн, по направлениям, отнесенным к их компетенции.

### 3. Меры по обеспечению безопасности персональных данных при их обработке

#### 3.1. Общее описание мер

3.1.1. Компания самостоятельно определяет состав, перечень и принимает правовые, организационные и технические меры, а также меры физической безопасности, необходимые и достаточные для обеспечения выполнения своих обязанностей как оператора ПДн по их защите от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн.

3.1.2. К правовым мерам относятся:

- назначение Компанией лиц, принимающих участие в обеспечении безопасности ПДн;
- издание Компанией локальных актов по вопросам обработки ПДн:
  - настоящего Положения;
  - Перечня обрабатываемых ПДн;
  - Перечня должностей работников Компании, допущенных к обработке ПДн;
  - Политики Компании в отношении обработки ПДн.
- регулирование отношений по поручению обработки ПДн третьим лицам на основании гражданско-правовых договоров;
- ознакомление работников Компании, непосредственно осуществляющих обработку ПДн, с требованиями к защите ПДн, локальными актами Компании по вопросам обработки ПДн.

3.1.3. К организационным мерам относятся:

- определение перечня ПДн, обрабатываемых в Компании (п. 3.2. настоящего Положения);
- издание локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации о ПДн, устранение последствий таких нарушений;
- ограничение доступа к ПДн и учет лиц, получивших доступ к ПДн (п. 3.3. настоящего Положения);
- учет машинных носителей ПДн;
- осуществление внутреннего аудита соответствия обработки ПДн требованиям к защите ПДн, Политике Компании в отношении обработки ПДн и иным локальным актам Компании по вопросам обработки ПДн;
- оценка вреда, который может быть причинен субъектам ПДн в случае нарушения безопасности ПДн, соотношение указанного вреда и принимаемых Компанией мер;
- определение актуальных угроз безопасности ПДн, обрабатываемых в ИСПДн;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы, обрабатывающей ПДн;
- проведение подготовки и периодического повышения осведомленности работников, которые в силу должностных обязанностей имеют доступ к ПДн в вопросах обеспечения безопасности ПДн;
- опубликование Политики в отношении обработки ПДн на официальном сайте Компании в сети Интернет.



3.1.4. Технические меры по обеспечению безопасности ПДн при их обработке в информационных системах Компании реализуются с помощью системы защиты ПДн, включающей средства защиты информации, а также используемые в информационной системе информационные технологии. Система защиты ПДн обеспечивает:

- требуемые уровни защищенности ПДн;
- предотвращение несанкционированного доступа к ПДн, в том числе случайного, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также регистрацию и учет всех действий, совершаемых с ПДн в информационной системе, обрабатывающей ПДн;
- постоянный контроль обеспечения уровня защищенности ПДн, обрабатываемых в информационных системах Компании.

Работы по обеспечению безопасности ПДн при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

Требования к техническим мерам и средствам защиты ПДн определяются на основании Модели угроз информационной безопасности Компании.

3.1.5. К мерам по обеспечению физической безопасности помещений, средств вычислительной техники и материальных носителей, относятся:

- обеспечение физической целостности периметров помещений Компании (отсутствие брешей в периметре или зон, позволяющих осуществить несанкционированное проникновение в помещение);
- физический доступ в помещения, в которых обрабатываются ПДн, ограничивается системой контроля доступа;
- работникам Компании предоставляется доступ в помещения, в которых обрабатываются ПДн, в соответствии со служебной необходимостью;
- нахождение посетителей, обслуживающего и технического персонала в помещениях, в которых обрабатываются ПДн, допускается только в присутствии работников Компании;
- по мере необходимости помещения оснащаются системой видеонаблюдения, охранной и тревожной сигнализацией.

## **3.2. Порядок определения Перечня персональных данных**

3.2.1. Перечень ПДн, обрабатываемых в Компании, утверждается Приказом Генерального директора. Обработка ПДн, не включенных в Перечень ПДн, обрабатываемых в Компании, запрещена.

3.2.2. Компания обрабатывает ПДн следующих категорий субъектов ПДн:

- представители юридического лица, индивидуальные предприниматели;
- клиенты - физические лица, заключившие с Компанией договор на брокерское и/или депозитарное обслуживание;

- контрагенты – физические лица, заключившие с Компанией договор гражданско-правового характера (за исключением договоров на брокерское и/или депозитарное обслуживание);
- кандидаты на вакантные места;
- работники Компании (в т.ч. уволенные);
- выгодоприобретатели по договорам добровольного страхования жизни работников Компании;
- аффилированные лица Компании;
- посетители.

3.2.3. Перечень ПДн, обрабатываемых в Компании, приведен в «Перечне персональных данных, обрабатываемых в ООО «Ренессанс Брокер»».

3.2.4. Обработке подлежат только такие ПДн и только в том составе, которые отвечают целям их обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

3.2.5. Целями обработки ПДн являются:

- исполнение договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также взаимодействие для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- обеспечение соблюдения требований действующего законодательства Российской Федерации, а также осуществление и выполнение возложенных действующим законодательством Российской Федерации на Компанию функций, полномочий и обязанностей;
- содействие работникам в трудоустройстве, обучении и продвижении по службе; обеспечение личной безопасности работников; контроль количества и качества выполняемой работы и обеспечение сохранности имущества;
- однократный пропуск субъектов ПДн на территорию Компании.

3.2.6. Срок хранения ПДн в зависимости от состава определяется:

- договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- федеральными законами;
- соглашением между Компанией и субъектом ПДн в случае, когда ПДн обрабатываются на основании согласия субъекта.

### **3.3. Порядок определения Перечня должностей работников, допущенных к обработке персональных данных**

3.3.1. Работники Компании имеют право получать доступ в ИСПДн или к материальным носителям, содержащим только ПДн, которые необходимы им для выполнения возложенных должностных обязанностей.

3.3.2. Перечень должностей работников, допущенных к обработке ПДн, включает:

- наименование структурного подразделения Компании и должности работника согласно утвержденной организационной структуре Компании;
- состав ПДн, к которым работнику предоставлен доступ, согласно Перечню ПДн, обрабатываемых в Компании.

3.3.3. Допускается ведение Перечня должностей работников, допущенных к обработке ПДн, в электронном виде при условии предоставления работникам доступа в ИСПДн только

на основании письменной заявки согласно правилам предоставления доступа к информационным ресурсам Компании.

3.3.4. Перечень должностей работников, допущенных к обработке ПДн, составляется руководителями структурных подразделений, согласуется с лицом, ответственным за организацию обработки ПДн, утверждается приказом Генерального директора Компании.

3.3.5. Перечень должностей работников, допущенных к обработке ПДн, пересматривается по мере необходимости (изменение организационно-штатной структуры, введение новых должностей и т.п.) лицом, ответственным за организацию обработки ПДн, на основании заявок руководителей структурных подразделений.

### **3.4. Порядок получения согласия субъектов на обработку персональных данных**

3.4.1. Согласие субъектов, ПДн которых обрабатываются в Компании, необходимо получать в следующих случаях:

- создание внутренних справочников и адресных книг Компании;
- при передаче ПДн третьим лицам;
- при трансграничной передаче ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн (страны, не являющиеся сторонами Конвенции о защите физических лиц при автоматизированной обработке ПДн и не включенные в перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн и обеспечивающих адекватную защиту прав субъектов ПДн).

3.4.2. Согласие на передачу ПДн работника должно быть получено в письменной форме. Согласие на передачу третьим лицам ПДн иных категорий субъектов может быть предоставлено субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме.

3.4.3. В случае трансграничной передачи ПДн на территорию государств, не осуществляющих адекватную защиту ПДн, необходимо получение согласия субъекта в письменной форме.

3.4.4. равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Для целей настоящего пункта равнозначным содержащему собственноручную подпись работника Компании согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного простой электронной подписью, где простой электронной подписью считается сочетание логина и пароля работника Компании в службе каталогов Active Directory.

3.4.5. Форма согласия на обработку ПДн утверждается приказом Генерального директора Компании.

3.4.6. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным.

3.4.7. В случае получения согласия на обработку ПДн от представителя субъекта ПДн, полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Компанией. Работник Компании считается уполномоченным лицом на предоставление согласия на передачу ПДн указанными им лицами на передачу принадлежащим им ПДн страховым компаниям в целях заключения договоров добровольного страхования

работников от несчастных случаев и болезней, согласно которым указанные работником лица выступают выгодоприобретателями.

3.4.8. Компания обрабатывает ПДн представителей юридических лиц, содержащиеся в доверенностях, выданных юридическим лицом. Такие доверенности могут содержать подпись представителя юридического лица и пункт о согласии на обработку ПДн в объеме и целях, указанных в доверенности.

3.4.9. Компания вправе осуществлять обработку ПДн следующих субъектов без их согласия:

- представителей юридических лиц, данные которых обрабатываются в целях осуществления и выполнения возложенных действующим законодательством Российской Федерации на Компанию функций, полномочий и обязанностей либо на основании доверенности, выданной юридическим лицом в соответствии с п. 3.4.8. настоящего Положения;
- клиентов и контрагентов Компании, выгодоприобретателей по договорам добровольного страхования работников Компании от несчастных случаев и болезней в целях исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- кандидатов на вакантные места, ПДн которых сделаны общедоступными субъектом ПДн;
- работников Компании (в т.ч. уволенных), аффилированных лиц Компании в целях осуществления и выполнения возложенных действующим законодательством Российской Федерации на Компанию функций, полномочий и обязанностей;
- посетителей Компании для осуществления прав и законных интересов Компании и достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы посетителей.

3.4.10. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных федеральным законом.

3.4.11. Компания вправе осуществлять обработку сведений о судимости за преступления в сфере экономической деятельности и/или преступления против государственной власти у лиц, входящих в состав совета директоров (наблюдательного совета), членов коллегиального исполнительного органа, единоличного исполнительного органа и контролера Компании в соответствии с требованиями Федерального закона от 22.04.1996 № 39 «О рынке ценных бумаг» без получения письменного согласия указанных лиц.

3.4.12. Согласие на обработку ПДн может быть отозвано субъектом ПДн. Порядок отзыва согласия субъекта на обработку ПДн определяется в согласии. В случае отзыва субъектом ПДн согласия на обработку ПДн Компания вправе продолжить обработку ПДн без согласия субъекта ПДн только при наличии следующих оснований:

- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных действующим законодательством Российской Федерации на Компанию функций, полномочий и обязанностей;

- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- обработка ПДн необходима для осуществления прав и законных интересов Компании или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- осуществляется обработка обезличенных ПДн;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

## **4. Порядок обработки персональных данных**

### **4.1. Принципы и правила обработки персональных данных**

4.1.1. Обработка ПДн Компанией осуществляется с соблюдением следующих принципов и правил:

- обработка ПДн должна осуществляться на законной и справедливой основе;
- обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;
- не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки;
- при обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Компания должна принимать необходимые меры, либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
- хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Место хранения ПДн определяется в соответствии с действующим законодательством.

### **4.2. Порядок предоставления доступа к персональным данным работникам Компании**

4.2.1. Работники Компании имеют право получить доступ к ИСПДн или к материальным носителям, содержащим ПДн, исключительно в объеме, который необходим для выполнения должностных обязанностей и должность которого включена в Перечень должностей работников, допущенных к обработке ПДн.

4.2.2. Работнику Компании, должность которого не включена в Перечень должностей работников, допущенных к обработке ПДн, но которому необходим разовый или временный доступ к ПДн субъектов в связи с исполнением должностных обязанностей, может быть предоставлен такой доступ на основании обоснованного письменного запроса руководителя структурного подразделения работника на имя лица, ответственного за организацию обработки ПДн, при условии выполнения требований п. 4.2.3. настоящего Положения.

4.2.3. Доступ работников Компании к ПДн предоставляется на базе «разрешительной системы», включающей следующие меры:

4.2.3.1. Компания обязана ознакомить под подпись работников, которым доступ к ПДн необходим для выполнения служебных обязанностей, со следующими документами:

- Политикой Компании в отношении обработки ПДн;
- настоящим Положением;
- Перечнем ПДн, обрабатываемых в Компании;
- Памяткой работника Компании, в должностные обязанности которого входит обработка ПДн (Приложение 1 к настоящему Положению).

4.2.3.2. Лица, ответственные за исполнение работниками структурных подразделений Компании требований к защите ПДн, обязаны довести до сведения работников структурных подразделений Компании требования к защите ПДн;

4.2.3.3. Подразделение, ответственное за реализацию мероприятий по защите ПДн, должно провести инструктаж и обучить работников, которые в силу своих служебных обязанностей имеют доступ к ИСПДн, использованию технических средств защиты информации.

4.2.4. Доступ в ИСПДн предоставляется на основании заявки пользователя или его руководителя с учетом требований п.4.2 настоящего Положения.

4.2.5. Доступ к машинным носителям ПДн предоставляется с учетом требований п.4.9. настоящего Положения.

4.2.6. Доступ работников Компании к ПДн подлежит пересмотру в следующих случаях:

- изменение должности работника или его функциональных обязанностей;
- перевод работника из одного структурного подразделения Компании в другое;
- увольнение работника;
- по результатам контроля выполнения требований по обработке ПДн.

### **4.3. Порядок сбора и уточнения персональных данных**

4.3.1. ПДн преимущественно предоставляются Компании лично субъектами ПДн (за исключением случаев, указанных в п. 4.3.2 настоящего Положения).

4.3.2. Компания вправе обрабатывать ПДн, полученные от лица, не являющегося субъектом ПДн, в следующих случаях:

- ПДн представителей юридического лица предоставлены юридическим лицом на основании федерального закона или в связи с исполнением договора с юридическим лицом;
- ПДн выгодоприобретателей по договорам страхования работников от несчастных случаев и болезней получены Компанией от работника в связи с исполнением договора, выгодоприобретателем по которому является субъект ПДн;
- ПДн кандидата сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- субъект ПДн уведомлен об осуществлении обработки его данных Компанией.

4.3.3. На субъекта ПДн может быть возложена обязанность по уточнению ПДн в случае их изменения.

4.3.4. При сборе персональных данных Компания осуществляет запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных,

находящихся на территории Российской Федерации, за исключением случаев, предусмотренных Российским законодательством.

#### **4.4. Порядок передачи и предоставления персональных данных. Обработка персональных данных третьими лицами**

4.4.1. Компания вправе поручить обработку ПДн третьим лицам только с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, существенными условиям которого являются:

- принципы и правила обработки ПДн;
- перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн;
- цели обработки ПДн;
- обязанность третьего лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;
- требования к защите обрабатываемых ПДн;
- порядок обеспечения Компанией прекращения обработки, уничтожения и блокирования ПДн лицом, осуществляющим обработку ПДн по договору.

4.4.2. Лицо, осуществляющее обработку ПДн по поручению Компании, не обязано получать согласие субъекта ПДн на обработку его ПДн.

4.4.3. Компания несет ответственность перед субъектом ПДн за действия лица, которому была поручена обработка ПДн субъекта. Лицо, осуществляющее обработку ПДн по поручению Компании, несет ответственность перед Компанией в соответствии с договором.

4.4.4. Лицо, осуществляющее обработку ПДн по поручению Компании, не вправе раскрывать третьим лицам и распространять ПДн, если иное не предусмотрено федеральным законом.

4.4.5. Компания вправе осуществлять передачу обезличенных ПДн без согласия субъекта ПДн.

4.4.6. Компания не осуществляет раскрытие обрабатываемых ПДн неопределенному кругу лиц (распространение ПДн).

#### **4.5. Порядок трансграничной передачи персональных данных**

4.5.1 Трансграничная передача данных в Компании осуществляется на следующих условиях:

- Выполнены требования п.3.4 настоящего документа.
- Осуществляется передача баз данных, содержащих ПДн, при сборе которых запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации производились с использованием баз данных, находящихся на территории Российской Федерации.
- Для выполнения возложенных действующим законодательством Российской Федерации на компанию требований.

## 4.6. Порядок обезличивания персональных данных

4.6.1. Обезличивание ПДн подразумевает действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту.

4.6.2. Компания применяет обезличивание ПДн работников, уволенных до подписания согласия на передачу ПДн третьим лицам для осуществления и выполнения возложенных действующим законодательством Российской Федерации на Компанию функций, полномочий и обязанностей как работодателя и налогового агента.

4.6.3. Обезличивание ПДн работников, уволенных до подписания согласия на передачу ПДн третьим лицам, выполняется путем исключения из перечня передаваемых ПДн фамилии, имени и отчества уволенного работника.

## 4.7. Порядок хранения и уничтожения персональных данных

4.7.1. ПДн хранятся в форме, позволяющей определить субъекта ПДн.

4.7.2. При хранении разделяются ПДн, созданные для несовместимых между собой целей обработки:

4.7.2.1. В случае автоматизированной обработки для каждой из целей обработки создаются обособленные базы данных ИСПДн.

4.7.2.2. В случае неавтоматизированной обработки ПДн, созданные для несовместимых между собой целей обработки, фиксируются на отдельных материальных носителях.

4.7.3. Сроки хранения ПДн, а также основания для обработки ПДн определяются в соответствии с п. 3.2.6 в Перечне ПДн, обрабатываемых в Компании.

4.7.4. Срок хранения ПДн начинает течь:

- для ПДн работников Компании – с момента расторжения трудового договора;
- для ПДн представителей юридических лиц, клиентов Компании – с момента прекращения отношений с клиентом;
- для ПДн контрагентов – с момента расторжения договора;
- для ПДн кандидатов на вакантные должности в Компании – с момента получения сведений о кандидате из общедоступных источников;
- для ПДн выгодоприобретателей по договорам страхования работников от несчастных случаев и болезней – с момента истечения срока действия договора или наступления страхового случая;
- для посетителей Компании – с момента выдачи одноразового пропуска.

4.7.5. Компания прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) и уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) в срок, не превышающий тридцати дней с даты истечения срока хранения ПДн.

4.7.6. Уничтожение ПДн в ИСПДн выполняется штатными средствами ИСПДн. Решение об уничтожении ПДн в ИСПДн принимает лицо, ответственное за организацию обработки ПДн и согласовывает:

- для ПДн представителей юридических лиц, клиентов и контрагентов Компании - с начальником Управления по работе с клиентами;



- для ПДн работников, кандидатов на вакантные должности в Компании, выгодоприобретателей по договорам страхования работников от несчастных случаев и болезней – с руководителем Управления по работе с персоналом.

К уничтожению ПДн в ИСПДн могут привлекаться работники подразделения, ответственного за реализацию мероприятий по защите ПДн.

4.7.7. Уничтожение материальных носителей ПДн выполняется в соответствии с п. 4.9. настоящего Положения.

#### **4.8. Порядок блокирования персональных данных**

4.8.1. Блокирование ПДн выполняется путем временного прекращения обработки данных средствами ИСПДн в случае автоматизированной и организационными мерами в случае неавтоматизированной обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

4.8.2. В случае автоматизированной обработки ПДн блокирование выполняется средствами ИСПДн подразделением, ответственным за реализацию мероприятий по защите ПДн, по поручению лица, ответственного за организацию обработки ПДн.

4.8.3. В случае неавтоматизированной обработки ПДн, ответственное за организацию обработки ПДн, сообщает лицам, ответственным за исполнение работниками структурных подразделений Компании, требований к защите ПДн, о необходимости временного прекращения обработки ПДн (запрет доступа к носителям ПДн, прекращение операций с ПДн). Лица, ответственные за исполнение работниками структурных подразделений Компании требований к защите ПДн, доводят до сведения работников структурного подразделения требования по временному прекращению обработки ПДн.

4.8.4. Блокирование ПДн выполняется в следующих случаях:

- ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- неправомерная обработка ПДн, выявленная при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн;
- отсутствует возможность уничтожения ПДн в течение требуемого срока.

#### **4.9. Порядок обращения с материальными носителями персональных данных**

4.9.1. Материальные носители (бумажные и машинные), содержащие ПДн, подлежат хранению в служебных помещениях в запираемых шкафах или сейфах, определенных в Перечне хранилищ носителей ПДн. При этом соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Форма Перечня хранилищ носителей ПДн приведена в Приложении 2.к настоящему Положению.

4.9.2. Не допускается оставление без присмотра материальных носителей ПДн, а также ключей от запираемых шкафов и сейфов.

4.9.3. Машинные носители (оптические диски, гибкие диски, жесткие диски, flash-накопители и другие устройства внешней памяти), содержащие ПДн, подлежат учету работниками подразделения, ответственного за реализацию мероприятий по защите ПДн. Учет носителей включает в себя маркировку, регистрацию выдачи и уничтожения носителя.

4.9.4. При учете каждому машинному носителю присваивается идентификационный номер и выполняется маркировка путем нанесения специальной наклейки, надписи

нестираемым маркером или иным способом, гарантирующим долговечность нанесенной надписи.

4.9.5. Выдача носителей ПДн работникам Компании осуществляется по запросу руководителя структурного подразделения работника. Выдача машинных носителей ПДн фиксируется в Журнале учета машинных носителей ПДн. Типовая форма Журнала учета машинных носителей, предназначенных для хранения ПДн, приведена в Приложении 3. К настоящему Положению. Допускается ведение Журнала учета машинных носителей в электронном виде.

4.9.6. Работники подразделения, ответственного за реализацию мероприятий по защите ПДн, осуществляют контроль машинных носителей, отправляемых на ремонт. Перед отправкой носителя на ремонт с него должны быть удалены все хранящиеся на нем ПДн способом, гарантирующим невозможность восстановления хранимых данных.

4.9.7. Машинные носители ПДн, подлежащие уничтожению или вышедшие из строя, передаются работниками Компании в подразделение, ответственное за реализацию мероприятий по защите ПДн.

4.9.8. Уничтожение машинных носителей ПДн должно осуществляться способом, исключающим возможность восстановления хранимой на машинном носителе ПДн информации, с использованием средств гарантированного уничтожения информации - специализированными программными средствами, путем физической деструкции носителя или воздействием внешнего магнитного поля.

4.9.9. По факту уничтожения носителя ПДн в Журнале учета машинных носителей ПДн ставится отметка о его уничтожении.

4.9.10. Уничтожение бумажных носителей ПДн, находящихся на архивном хранении, осуществляется согласно принятым в Компании правилам архивного документооборота.

4.9.11. Бумажные носители ПДн, не подлежащие архивному хранению согласно актам Компании, должны быть уничтожены работниками Компании, в распоряжении которых находятся такие носители, непосредственно после использования согласно п. 4.9.13. настоящего Положения.

4.9.12. Для уничтожения бумажных носителей ПДн, находящихся в текущем оперативном хранении, срок хранения которых истек, в Компании формируется экспертная комиссия. Экспертная комиссия производит выделение к уничтожению и уничтожение бумажных носителей ПДн, срок хранения которых истек, по результатам которого составляется акт о выделении к уничтожению и уничтожении бумажных носителей ПДн, не подлежащих хранению. Форма акта приведена в Приложении 4. к настоящему Положению.

4.9.13. Бумажные носители ПДн уничтожаются путем сожжения/ дробления/ измельчения (с использованием шредера)/ иным способом.

#### **4.10. Порядок неавтоматизированной обработки персональных данных**

4.10.1. ПДн при их обработке, осуществляемой без использования средств вычислительной техники, должны обособляться от иной информации, в частности, путем фиксации их на отдельных носителях.

4.10.2. В случае, если на одном материальном носителе зафиксированы ПДн с разными целями обработки и носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, принимаются меры по обеспечению раздельной обработки ПДн, в частности:

4.10.2.1. при необходимости использования или передачи определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн, осуществляется копирование необходимых ПДн способом, исключающим одновременное копирование других ПДн, и используется (передается) копия ПДн;

4.10.2.2. при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

4.10.3. Уточнение ПДн при осуществлении их обработки без использования средств вычислительной техники производится путем обновления или изменения данных на материальном носителе. Если это не допускается техническими особенностями материального носителя, то уточнение производится путем фиксации на том же материальном носителе сведений о вносимых в ПДн изменениях, либо путем изготовления нового материального носителя с уточненными ПДн.

4.10.4. При использовании для неавтоматизированного сбора или уточнения ПДн типовых форм документов, соблюдаются следующие условия:

4.10.4.1. типовая форма документа или связанные с ней документы (инструкция по ее заполнению, приложения, карточки, реестры и журналы) должны содержать:

- сведения о цели обработки ПДн;
- наименование и адрес Компании;
- фамилию, имя, отчество и адрес субъекта ПДн;
- источник получения ПДн;
- сроки обработки ПДн;
- перечень действий с ПДн, которые будут совершаться в процессе их обработки;
- общее описание используемых Компанией способов обработки ПДн.

4.10.4.2. типовая форма документа должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн (в случае, когда это согласие требуется). Типовая форма документа должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

4.10.4.3. типовая форма документа должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

## **5. Права и обязанности сторон**

### **5.1. Права субъектов персональных данных**

5.1.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Компанией;
- правовые основания и цели обработки ПДн;

- цели и применяемые Компанией способы обработки ПДн;
- наименование и место нахождения Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Компанией или на основании федеральных законов;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральными законами;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- информацию об осуществленной или предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Компании, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами.

5.1.2. Сведения, указанные в п. 5.1.1. настоящего Положения, предоставляются субъекту ПДн или его представителю при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать:

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

Типовая форма запроса субъекта ПДн приведена в Приложении 5 к настоящему Положению.

5.1.3. При осуществлении субъектом ПДн своих прав через законного представителя, представитель должен предоставить доверенность от субъекта ПДн, заверенную нотариально или иным образом в соответствии с действующим законодательством Российской Федерации. Доверенность, выданная работником, составленная и подписанная в присутствии работника Управления по работе с персоналом, не требует нотариального заверения.

5.1.4. В случае, если сведения, указанные в п. 5.1.1. настоящего Положения, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно в Компанию или направить повторный запрос в целях получения сведений, указанных в п. 5.1.1. настоящего Положения и ознакомления с такими ПДн не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральными законами, принятым в соответствии с ними нормативными правовыми актами или договором, стороной которого или выгодоприобретателем или поручителем по которому является субъект ПДн.

5.1.5. Субъект ПДн вправе обратиться повторно в Компанию или направить повторный запрос в целях получения сведений указанных в п. 5.1.1. настоящего Положения, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в п. 5.1.4. настоящего Положения в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п.

5.1.2. настоящего Положения, должен содержать обоснование направления повторного запроса.

5.1.6. Субъект ПДн вправе требовать от Компании уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.1.7. Если субъект ПДн считает, что Компания осуществляет обработку его ПДн с нарушением требований федеральных законов или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Компании в уполномоченном органе по защите прав субъектов ПДн или в судебном порядке.

5.1.8. Субъект ПДн имеет право отозвать свое согласие на обработку ПДн, предоставленное в случаях, указанных в п. 3.4. настоящего Положения.

5.1.9. Субъект ПДн имеет право на обжалование действий или бездействия Компании и на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда, в судебном порядке.

5.1.10. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, установленных федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», а также требований к защите ПДн, подлежит возмещению в соответствии с действующим законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.

5.1.11. В дополнение к правам субъектов ПДн, указанных в пп. 5.1.1. - 5.1.10. настоящего Положения в целях обеспечения защиты ПДн, хранящихся в Компании, работники имеют право на:

- полную информацию об их ПДн и обработке этих данных;
- свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн работника, за исключением случаев, предусмотренных федеральным;
- определение своих представителей для защиты своих ПДн;
- требование об исключении или исправлении неверных или неполных ПДн, а также данных, обработанных с нарушением требований федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Трудового Кодекса Российской Федерации или иного федерального закона. При отказе Компании исключить или исправить ПДн работника он вправе заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия. ПДн оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении Компанией всех лиц, которым ранее были сообщены неверные или неполные ПДн работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия Компании при обработке и защите ПДн.

## 5.2. Права и обязанности Компании как оператора персональных данных

5.2.1. Компания обязана принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей по защите ПДн в соответствии с п. 3.1. настоящего Положения.

5.2.2. Компания обязана предоставить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

5.2.3. Сведения, указанные в п. 5.1.1. настоящего Положения, должны быть предоставлены субъекту ПДн Компанией в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

5.2.4. Компания вправе мотивированно отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным п. 5.1.5. настоящего Положения.

5.2.5. По факту обращения или получения запроса от субъекта ПДн или его законного представителя:

5.2.5.1. Компания обязана безвозмездно и в доступной форме сообщить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя;

5.2.5.2. В случае отказа Компания в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя, обязана предоставить в письменной форме мотивированный отказ, содержащий ссылку на федеральный закон, ограничивающий право субъекта на доступ к его ПДн, в том числе если:

- обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

5.2.5.3. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя Компания обязана:

- в случае предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными:
  - внести изменения в ПДн субъекта в срок, не превышающий семи рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя;
  - обеспечить уточнение ПДн (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) в течение семи рабочих дней со дня представления таких сведений;
  - принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы;
  - уведомить субъекта о внесенных изменениях и предпринятых мерах.

5.2.5.4. В случае представления субъектом или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки Компания обязана:

- уничтожить ПДн в срок, не превышающий семи рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя;
- принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы;
- уведомить субъекта о внесенных изменениях и предпринятых мерах.

5.2.5.5. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя Компания обязана:

- осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) с момента такого обращения или получения указанного запроса на период проверки;
- если в результате проверки подтвердится факт неправомерной обработки ПДн, осуществляемой Компанией или лицом, действующим по поручению Компании, Компания в срок, не превышающий трех рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Компании;
- если обеспечить правомерность обработки ПДн невозможно, Компания в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязана уничтожить такие ПДн или обеспечить их уничтожение;
- об устранении допущенных нарушений или об уничтожении ПДн Компания обязана уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

К неправомерной обработке ПДн относится:

- обработка ПДн, осуществляемая с нарушением принципа законности и справедливости основания обработки;
- обработка ПДн, несовместимая с целями сбора ПДн;
- содержание и объем обрабатываемых ПДн, не соответствующие заявленным целям обработки;
- обработка ПДн по достижении целей обработки или в случае утраты необходимости в их достижении;
- объединение баз данных ИСПДн, созданных для несовместимых между собой целей.

5.2.5.6. В случае отзыва субъектом ПДн согласия на обработку его ПДн Компания обязана:

- прекратить обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании);
- в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено

договором (иным соглашением), стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

5.2.5.7. В случае отсутствия возможности уничтожения ПДн в течение требуемого срока, Компания осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральным законом.

5.2.5.8. В случае достижения цели обработки ПДн Компания обязана прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Компанией и субъектом ПДн либо если Компания не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

5.2.5.9. Компания обязана сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

### **5.3. Обязанности работников Компании в части защиты и хранения ПДн**

5.3.1. Работники Компании, которые в силу своих служебных обязанностей имеют доступ к ПДн, обязаны:

- знать и выполнять требования законодательства Российской Федерации о ПДн, настоящего Положения и иных локальных актов Компании по вопросам обработки ПДн;
- принимать меры по защите ПДн или по обеспечению безопасности ПДн;
- при уходе в отпуск, служебной командировке, иных случаях длительного отсутствия на своем рабочем месте или увольнении, работник обязан передать материальные носители, содержащие ПДн, другому работнику по указанию руководителя структурного подразделения с учетом требований п. 4.2. настоящего Положения;
- незамедлительно ставить в известность лицо, ответственное за организацию обработки ПДн, об утрате или недостатке материальных носителей ПДн, паролей доступа, удостоверений, пропусков, ключей от помещений и хранилищ, сейфов и о других фактах, которые могут привести к разглашению ПДн, а также о причинах и условиях возможной утечки ПДн;
- незамедлительно ставить в известность лицо, ответственное за организацию обработки ПДн, о попытках посторонних лиц получить от работника ПДн, обрабатываемые Компанией.

5.3.2. Все Работники Компании обязаны использовать аппаратные и программные средства Компании исключительно в связи с исполнением ими своих трудовых обязанностей. Работникам не допустимо размещать, пересылать и хранить личные ПДн с использованием аппаратных и программных средств Компании.



## **6. Порядок взаимодействия с субъектами персональных данных и уполномоченным органом по защите прав субъектов**

### **6.1. Общие правила взаимодействия с субъектами персональных данных**

6.1.1. Субъекты ПДн и их представители вправе обратиться в Компанию или направить запрос следующими способами:

- лично к лицу, ответственному за организацию обработки ПДн в Компании (только работники Компании);
- путем направления почтового сообщения на адрес Компании;
- путем направления электронного сообщения в форме электронного документа, подписанного квалифицированной электронной подписью в соответствии с законодательством Российской Федерации.

6.1.2. В случае взаимодействия с субъектами ПДн путем обмена сообщениями должна обеспечиваться конфиденциальность передаваемых данных:

- в случае направления субъекту ПДн почтового сообщения (заказного письма) через организацию Федеральной почтовой связи в целях обеспечения конфиденциальности должны использоваться светонепроницаемые конверты или вложения должны быть обернуты светонепроницаемой бумагой. На конверт наносятся только реквизиты, предусмотренные почтовыми правилами для почтовых отправлений, далее конверт передается в подразделение, ответственное за прием и отправку почтовой корреспонденции, для отправки;
- в случае направления субъекту ПДн электронного сообщения должна использоваться электронная подпись.

6.1.3. Не допускается отвечать на запросы субъектов ПДн или их законных представителей, связанные с предоставлением ПДн, по телефону или факсу.

6.1.4. Запросы субъектов ПДн на предоставление сведений об обработке их ПДн должны регистрироваться лицом, ответственным за организацию обработки ПДн, в Журнале учета обращений субъектов ПДн и уполномоченного органа по вопросам обработки ПДн (далее – Журнал). Типовая форма Журнала приведена в Приложении 6 к настоящему Положению.

### **6.2. Порядок реагирования на запросы субъектов персональных данных**

6.2.1. Устанавливается следующий порядок взаимодействия лиц, ответственных за взаимодействие с субъектами ПДн, при получении запроса от субъекта:

6.2.1.1. В случае личного обращения работника Компании к лицу, ответственному за организацию обработки ПДн в Компании, работник заполняет типовую форму запроса в соответствии с п. 5.1.2. настоящего Положения;

6.2.1.2. В случае письменного обращения на почтовый адрес Компании первоначальную обработку запросов от субъектов ПДн осуществляет организационное подразделение, ответственное за прием и отправку почтовой корреспонденции. Запрос регистрируется в соответствии с правилами документооборота Компании и передается лицу, ответственному за организацию обработки ПДн в течение одного рабочего дня.

6.2.1.3. В случае направления субъектом ПДн электронного сообщения, такое сообщение должно быть передано лицу, ответственному за организацию обработки ПДн в Компании, в течение одного рабочего дня.

6.2.2. Лицо, ответственное за организацию обработки ПДн, в случае получения запроса субъекта ПДн регистрирует запросы субъектов ПДн в Журнале.

6.2.3. В случае возникновения у лица, ответственного за организацию обработки ПДн, обоснованных сомнений в правомочности запроса или легитимности доверенности представителя субъекта ПДн:

6.2.3.1. запрос передается на экспертизу в подразделение, ответственное за юридическое обеспечение деятельности по защите ПДн;

6.2.3.2. в случае если запрос признан не правомочным, работник подразделения, ответственного за юридическое обеспечение деятельности по защите ПДн, составляет ответ, содержащий обоснованный отказ, и направляет его лицу, ответственному за организацию обработки ПДн;

6.2.3.3. в случае если запрос признан правомочным, работник подразделения, ответственного за юридическое обеспечение деятельности по защите ПДн, направляет заключение экспертизы лицу, ответственному за организацию обработки ПДн, для обеспечения подготовки ответа на запрос;

6.2.3.4. юридическая экспертиза должна быть выполнена в течение трех рабочих дней.

6.2.4. В случае запроса на предоставление сведений об обработке ПДн:

6.2.4.1. лицо, ответственное за организацию обработки ПДн, передает запрос лицам, ответственным за исполнение работниками структурных подразделений Компании требований к защите ПДн, для назначения исполнителя подготовки ответа на запрос субъекта;

6.2.4.2. назначенный исполнитель готовит ответ на запрос субъекта с соблюдением сроков, указанных лицом, ответственным за организацию обработки ПДн. Типовая форма ответа на запрос субъекта на предоставление сведений об обработке ПДн приведена в Приложении 7 к настоящему Положению.

6.2.4.3. подготовленный ответ направляется лицу, ответственному за организацию обработки ПДн.

6.2.5. В случае запроса на блокирование, уточнение, изменение, уничтожение ПДн в ИСПДн Компании:

6.2.5.1. лицо, ответственное за организацию обработки ПДн направляет запрос в подразделение, ответственное за реализацию мероприятий по защите ПДн;

6.2.5.2. работник подразделения, ответственного за реализацию мероприятий по защите ПДн, предпринимает меры в соответствии с положениями п. 5.2.5 настоящего Положения;

6.2.5.3. по факту выполнения запроса исполнитель подготавливает уведомление о проделанных операциях и направляет его лицу, ответственному за организацию обработки ПДн.

6.2.6. Получив подготовленный ответ, лицо, ответственное за организацию обработки ПДн:

6.2.6.1. регистрирует действия по результатам обращения в Журнале;

6.2.6.2. в случае личного обращения, вручает ответ в руки работнику Компании;

6.2.6.3. в случае письменного запроса на адрес Компании, передает ответ в организационное подразделение, ответственное за прием и отправку почтовой корреспонденции, для передачи субъекту ПДн с учетом требований п. 6.1.2. настоящего Положения.

6.2.6.4. в случае электронного запроса, направляет ответ субъекту ПДн с учетом требований п. 6.1.2. настоящего Положения.

### **6.3. Общие сведения о деятельности уполномоченного органа в рамках государственного контроля и надзора**

6.3.1. Уполномоченным органом по защите прав субъектов ПДн является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор).

6.3.2. Операторы ПДн до начала обработки ПДн обязаны уведомить Роскомнадзор о намерении осуществлять обработку ПДн. Компания вправе осуществлять без уведомления Роскомнадзора обработку ПДн:

- работников Компании (в т.ч. уволенных) и аффилированных лиц Компании, ПДн которых обрабатываются в соответствии с трудовым законодательством;
- представителей юридического лица, клиентов Компании, контрагентов, а также выгодоприобретателей по договорам добровольного страхования работников Компании от несчастных случаев и болезни, полученных Компанией в связи с заключением договора, стороной или выгодоприобретателем которого является субъект ПДн, т.к. ПДн не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются Компанией исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;
- кандидатов на вакантные места, ПДн которых сделаны общедоступными субъектом ПДн, или получены из общедоступных источников;
- посетителей Компании, ПДн которых обрабатываются Компанией в целях однократного пропуска субъекта ПДн на территорию Компании или в иных аналогичных целях.

6.3.3. Если субъект ПДн считает, что Компания осуществляет обработку его ПДн с нарушением требований законодательства Российской Федерации о ПДн или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Компании в Роскомнадзор или в судебном порядке.

6.3.4. По запросу Роскомнадзора Компания обязана представить документы и локальные акты, и (или) иным образом подтвердить принятие мер, направленных на обеспечение выполнения Компанией обязанностей, предусмотренных законодательством в области ПДн.

6.3.5. Компания обязана сообщить в Роскомнадзор по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

6.3.6. В случае наличия у Роскомнадзора предположений о нарушениях Компанией законодательства Российской Федерации о ПДн, допущенных при обработке ПДн, по уточнению, блокированию и уничтожению ПДн, Роскомнадзор вправе в интересах неограниченного количества субъектов ПДн направлять запросы на их устранение. Обязанности Компании по реагированию на такие запросы аналогичны описанным в п. 5.2.5. настоящего Положения. Запросы Роскомнадзора по вопросам обработки ПДн субъектов должны регистрироваться в Журнале.

6.3.7. В рамках государственного контроля и надзора Роскомнадзор вправе осуществлять плановые и внеплановые проверки Компании в документарной или выездной форме.

6.3.8. По результатам проверки должностными лицами Роскомнадзора, составляется акт проверки, который оформляется непосредственно после ее завершения. Форма акта утверждена Приказом Минэкономразвития Российской Федерации от 30.04.2009 № 141.

6.3.9. По окончании проверки должностное лицо Роскомнадзора в журнале Компании по учету проверок производит запись о проведенной проверке. Форма Журнала учета проверок Компании, проводимых органами государственного контроля (надзора), органами муниципального контроля приведена в Приложении 8 к настоящему Положению.

#### **6.4. Порядок действий в рамках проверок уполномоченного органа**

6.4.1. При получении уведомления о проверке, подразделение, ответственное за прием и отправку почтовой корреспонденции, обязано в течение одного рабочего дня передать уведомление лицу, ответственному за организацию обработки ПДн.

6.4.2. В случае, если лицо, ответственное за организацию обработки ПДн, не может присутствовать при проведении выездной проверки в установленные Роскомнадзором сроки, Компания вправе обратиться в соответствующий территориальный орган Роскомнадзора с просьбой о переносе сроков проведения проверки.

6.4.3. Уведомление Роскомнадзора о выездной проверке включает:

- Приказ о проведении проверки;
- Программу проведения проверки, содержащую:
  - перечень требований законодательства Российской Федерации о ПДн, в отношении которых будет осуществляться проверка;
  - перечень документов, которые будут запрошены у Компании при проведении проверки;
  - мероприятия, которые будут выполнены при проведении проверки.

6.4.4. Уведомление Роскомнадзора о документарной проверке включает перечень документов, которые требуется предоставить в рамках проверки.

6.4.5. Получив уведомление о проверке, лицо, ответственное за организацию обработки ПДн, в течение двух рабочих дней (в случае плановой проверки), либо одного рабочего дня (в случае внеплановой проверки):

- уведомляет руководство Компании и лиц, указанных в п. 2 настоящего Положения о виде и сроках проведения проверки;
- привлекает подразделение, ответственное за юридическое обеспечение деятельности по защите ПДн, для юридической экспертизы:
  - соответствия приказа о проведении проверки приложению 1 Приказа Минэкономразвития Российской Федерации от 30.04.2009 № 141;
  - законности заявленных целей проведения проверки, предмета проверки, правовых оснований поведения проверки;
  - соответствия запрашиваемых документов, предметной области обеспечения безопасности ПДн;
- организует сбор документов, которые требуется предоставить в ходе проверки.

6.4.6. Перечень документов, которые могут быть запрошены в рамках проведения проверок, приведен в таблице 1.

Таблица 1 – Перечень документов, которые могут быть запрошены в рамках проведения проверок уполномоченным органом по защите прав субъектов ПДн.

Типы документов	Наименование документов Компании	Ответственные за предоставление документов
Документы Компании, устанавливающие организационно-правовую форму, права и обязанности	<ul style="list-style-type: none"> <li>Устав Компании;</li> <li>Свидетельство о внесении записи в ЕГРЮЛ;</li> <li>Лицензии на осуществление деятельности на рынке ценных бумаг</li> </ul>	Подразделение, ответственное за юридическое обеспечение деятельности по защите ПДн
Документы, используемые при осуществлении деятельности по обработке ПДн и связанные с исполнением обязательных требований, установленных законодательством Российской Федерации о ПДн	<ul style="list-style-type: none"> <li>Журнал учета обращений субъектов ПДн;</li> <li>Типовые формы договоров с третьими лицами, содержащие пункт о поручении обработки ПДн;</li> <li>Перечень хранилищ носителей ПДн;</li> <li>Типовые формы документов, подразумевающие включение ПДн</li> </ul>	Лицо, ответственное за организацию обработки ПДн
<ul style="list-style-type: none"> <li>Акты предыдущих проверок в области ПДн, материалы рассмотрения дел об административных правонарушениях и иные документы о результатах, проведенных в отношении Компании проверок за соответствием обработки ПДн требованиям законодательства Российской Федерации о ПДн</li> <li>Документы, подтверждающие выполнение Компанией предписаний об устранении ранее выявленных нарушений законодательства Российской Федерации о ПДн</li> </ul>	<i>Применимо если ранее в отношении Компании проводились проверки</i>	Лицо, ответственное за организацию обработки ПДн
Уведомление об обработке ПДн	Копия уведомления об обработке персональных данных, направленное в уполномоченный орган по защите прав субъектов персональных данных	Лицо, ответственное за организацию обработки ПДн
Документы, необходимые для проверки фактов, содержащих признаки нарушения законодательства Российской Федерации о ПДн, изложенные в	<i>Определяются в ходе проверки</i>	Лицо, ответственное за организацию обработки ПДн

Типы документов	Наименование документов Компании	Ответственные за предоставление документов
обращения граждан и информации, поступившей в Роскомнадзор		
Письменное согласие субъекта ПДн на обработку его ПДн	Согласие работника на обработку ПДн	Лицо, ответственное за организацию обработки ПДн
Документы, подтверждающие соблюдение требований законодательства Российской Федерации при обработке специальных категорий и биометрических ПДн	<i>Не применимо к Компании</i>	-
Документы, подтверждающие уничтожение Компанией ПДн субъектов по достижении цели обработки	<ul style="list-style-type: none"> <li>• Журнал учета машинных носителей ПДн;</li> <li>• Акт о выделении к уничтожению бумажных носителей ПДн</li> </ul>	Лицо, ответственное за организацию обработки ПДн
Локальные акты Компании по вопросам обработки ПДн	<ul style="list-style-type: none"> <li>• Политика Компании в отношении обработки ПДн;</li> <li>• Положение о ПДн</li> </ul>	Лицо, ответственное за организацию обработки ПДн
Исследование (обследование) информационной системы ПДн, в части касающейся ПДн субъектов, обрабатываемых в ней	<ul style="list-style-type: none"> <li>• Отчет об обследовании ИСПДн</li> </ul>	Лицо, ответственное за организацию обработки ПДн; лица, ответственные за исполнение работниками структурных подразделений Компании требований к защите ПДн

Указанные документы представляются в виде копий, заверенных печатью Компании и подписью Генерального директора или иного уполномоченного представителя Компании.

6.4.7. В случае документарной проверки:

6.4.7.1. Ответственные за предоставление документов (3 столбец таблицы 1) в течение пяти рабочих дней с момента получения уведомления:

- подготавливают копии запрошенных документов;
- передают копии запрошенных документов лицу, ответственному за организацию обработки ПДн.

6.4.7.2. Лицо, ответственное за организацию обработки ПДн, в течение двух рабочих дней со дня предоставления запрошенных документов:

- подготавливает ответ на запрос Роскомнадзора, в котором дает комментарии относительно документов, направляемых в Роскомнадзор, и дает прочие разъяснения;
- заверяет копии полученных документов печатью Компании и подписью Генерального директора;
- передает подготовленный комплект документов в подразделение, ответственное за прием и отправку почтовой корреспонденции.

6.4.7.3. Подразделение, ответственное за прием и отправку почтовой корреспонденции, в течение одного рабочего дня после передачи комплекта документов:

- направляет подготовленный комплект документов письмом с уведомлением о вручении на адрес местонахождения соответствующего территориального органа Роскомнадзора и на имя соответствующего уполномоченного на проведение проверки лица (указанного в пункте 2 приказа о проведении проверки, направляемого вместе с уведомлением).

6.4.7.4. В случае обнаружения должностным лицом Роскомнадзора ошибок, несоответствий и противоречий в предоставленных документах, в Компанию направляется запрос на разъяснения в части предоставленных документов. Предоставление требуемых разъяснений выполняется ответственными лицами в порядке аналогичном пп. 6.4.7.1 - 6.4.7.3 настоящего Положения

6.4.8. В случае выездной проверки:

6.4.8.1. Ответственные за предоставление документов (3 столбец таблицы 1) не менее чем за пять рабочих дней до дня начала проверки:

- подготавливают копии запрошенных документов;
- передают копии запрошенных документов лицу, ответственному за организацию обработки ПДн.

6.4.8.2. Лицо, ответственное за организацию обработки ПДн:

- обеспечивает необходимые условия для проведения проверки;
- лично сопровождает должностных лиц Роскомнадзора в течение периода проведения проверки;
- представляет документы, запрашиваемые должностными лицами Роскомнадзора;
- предоставляет иную информацию, необходимую для достижения целей проверки;
- обеспечивает доступ должностных лиц Роскомнадзора на территорию, в используемые Компанией при осуществлении обработки ПДн здания, строения, сооружения, помещения;
- предпринимает меры по устранению в ходе проверки обнаруженных несоответствий и нарушений.

## **7. Контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных**

### **7.1. Общие положения о порядке проведения мероприятий по мониторингу и контролю обработки персональных данных**

7.1.1. Мониторинг процессов обработки ПДн и контроль принимаемых мер по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн осуществляется путем проведения:

- периодических контрольных мероприятий;
- служебных расследований по фактам произошедших инцидентов информационной безопасности;
- внешних аудитов соответствия процессов обработки ПДн требованиям законодательства по защите ПДн при необходимости получения объективной и непредвзятой оценки соответствия процессов обработки ПДн требованиям законодательства Российской Федерации.

7.1.2. Ежегодно лицо, ответственное за организацию обработки ПДн, направляет Генеральному директору Компании и иным заинтересованным лицам отчет о проделанных мероприятиях по мониторингу и контролю обработки ПДн, включающий перечень предложений по совершенствованию организационных мер по обеспечению безопасности ПДн и системы защиты ПДн.

## **7.2. Порядок проведения периодических контрольных мероприятий**

7.2.1. В рамках периодических контрольных мероприятий проводятся:

- ежегодные плановые проверки соблюдения правил обработки ПДн (далее – внутренние проверки);
- внеплановые проверки в отношении определенного структурного подразделения Компании по решению лица, ответственного за организацию обработки ПДн.

7.2.2. Контрольные мероприятия проводятся в соответствии с разрабатываемой лицом, ответственным за организацию обработки ПДн, программой мероприятия, определяющей состав проверок, сроки проведения контрольного мероприятия, формат предоставления свидетельств и оформления результатов. Контрольные мероприятия проводятся лицом, ответственным за организацию обработки ПДн. Также вопросы соблюдения требований федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных и принятых в соответствии с ним нормативных актов» включаются в программы проверок, осуществляемых Отделом внутреннего аудита.

7.2.3. Руководители структурных подразделений Компании, в рамках которых запланировано проведение внутренних проверок, должны быть уведомлены об этом не менее чем за две недели до начала проверки.

7.2.4. Руководители структурных подразделений Компании, в рамках которых планируется проведение внеплановых проверок, должны быть уведомлены об этом не менее чем за три рабочих дня до начала проверки.

7.2.5. В рамках внутренних проверок должно быть выполнено:

7.2.5.1. проверка наличия и актуальности следующих учетных документов:

- Журнала учета обращений субъектов ПДн;
- Перечень хранилищ носителей ПДн;
- Журнал учета машинных носителей ПДн;
- Актов о выделении к уничтожению и уничтожении бумажных носителей ПДн, не подлежащих хранению.

7.2.5.2. проверка осведомленности работников Компании в области требований законодательства Российской Федерации о ПДн, локальных актов Компании по вопросам обработки ПДн, в том числе требований к защите ПДн;

7.2.5.3. проверка соответствия Перечня должностей работников, допущенных к обработке ПДн, фактическому состоянию;

7.2.5.4. проверка соответствия Перечня ПДн, обрабатываемых в Компании, фактическому состоянию;

7.2.5.5. проверка соблюдения правил допуска работников к ПДн и предоставления доступа к ИСПДн;

7.2.5.6. актуализация перечня угроз в Модели угроз безопасности ПДн;



7.2.5.7. проверка соответствия организационно-распорядительной документации по обеспечению безопасности ПДн требованиям законодательства Российской Федерации о ПДн;

7.2.5.8. проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности ПДн, в соответствии с требованиями эксплуатационной и технической документации.

7.2.6. Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально в виде отчета.

### **7.3. Порядок проведения служебных расследований**

7.3.1. Служебные расследования в обязательном порядке проводятся в следующих случаях:

7.3.1.1. выявление в ходе периодических контрольных мероприятий или внешних аудитов следующих нарушений:

- нарушение конфиденциальности, целостности, доступности ПДн;
- халатность и несоблюдение требований по обеспечению безопасности ПДн;
- несоблюдение условий хранения, использования, уничтожения носителей ПДн;
- иных фактов, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;

7.3.1.2. получение от руководителей структурных подразделений сведений о ставших им известными фактах нарушения правил обработки ПДн, об утрате или недостатке материальных носителей ПДн, удостоверений, пропусков, ключей от помещений и хранилищ, сейфов и о других фактах, которые могут привести к нарушению характеристик безопасности ПДн, а также о причинах и условиях таких нарушений;

7.3.1.3. получение жалоб от субъектов ПДн о нарушении законных прав и интересов в части обработки ПДн.

7.3.1.4. Лицо, ответственное за организацию обработки ПДн, доводит до сведения Генерального директора Компании о необходимости проведения служебного расследования. Решение о проведении служебного расследования принимает Генеральный директор Компании.

7.3.2. Генеральный директор Компании назначает комиссию для проведения служебного расследования (далее – Комиссия), в том числе председателя Комиссии, а также определяет срок проведения служебного расследования. Срок проведения служебного расследования не должен превышать один календарный месяц.

7.3.3. В состав Комиссии должно входить не менее трех работников Компании, включая:

- лицо, ответственное за организацию обработки ПДн;
- работник подразделения, ответственного за реализацию мероприятий по защите ПДн;
- руководитель структурного подразделения, в пределах которого было выявлено нарушение (если применимо);
- иные работники Компании по усмотрению Генерального директора Компании.

7.3.4. Задачами служебного расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению;
- предложение рекомендаций по устранению последствий нарушения;
- предложение рекомендаций по предотвращению совершения подобных нарушений.

7.3.5. По результатам служебного расследования председатель Комиссии составляет акт, который подписывается всеми членами Комиссии. Акт о результатах служебного расследования утверждается Генеральным директором Компании.

7.3.6. В случае получения достаточных данных о наличии вины в действиях работника Компании, в отношении которого проводилось служебное расследование, Генеральный директор Компании принимает решение о привлечении виновного к дисциплинарной или иной ответственности в соответствии с трудовым законодательством Российской Федерации.

7.3.7. В случае если в ходе служебного расследования были установлены факты готовящихся либо совершенных преступлений, Компания обязана немедленно сообщить об этом в соответствующие государственные органы.

## 7.4. Порядок проведения внешних аудитов

7.4.1. При необходимости получения объективной и непредвзятой оценки соответствия процессов обработки ПДн требованиям законодательства Российской Федерации о ПДн по представлению лица, ответственного за организацию обработки ПДн, утвержденному Генеральным директором Компании, может проводиться внешний аудит с привлечением сторонней организации.

7.4.2. К сторонней организации, привлекаемой для проведения аудита соответствия процессов обработки ПДн требованиям законодательства Российской Федерации о ПДн, предъявляются следующие требования:

- наличие в штате специалистов, получивших профильное образование в области защиты информации и/или информационных технологий либо прошедших аналогичные курсы повышения квалификации;
- опыт проведения работ в области защиты информации, информационных технологий и аудита.

7.4.3. Привлеченная к проведению аудита организация несет ответственность за:

- объективность и достоверность заключения по результатам аудита;
- соблюдение конфиденциальности сведений и документов, получаемых и составляемых в ходе аудита.

7.4.4. Требования к порядку получения, передачи, хранения и уничтожения документов Компании в рамках аудита и отчету по результатам аудита соответствия должны определяться договором на проведение аудита соответствия. С привлеченной к проведению аудита организацией должно быть заключено соглашение о конфиденциальности.

7.4.5. При проведении внешнего аудита в качестве основных источников при сборе свидетельств аудита должны использоваться:

- организационно-распорядительная документация Компании по обеспечению безопасности ПДн;
- сведения о технических средствах защиты ПДн;

- устные и письменные ответы работников Компании, полученные в процессе проводимых опросов;
- результаты наблюдений аудиторов за деятельностью Компании в области обработки и защиты ПДн.

7.4.6. По результатам проведения аудита аудиторской группой должен быть подготовлен отчет. Отчет должен содержать полные, точные, четкие и достаточные записи по аудиту и включать:

- сведения об объекте аудита;
- сведения о привлеченной организации;
- сведения о составе аудиторской группы;
- цели аудита;
- критерии аудита;
- область аудита, в частности, сведения о проверенных структурных подразделениях Компании и/или процессах;
- сроки проведения аудита;
- выводы аудита по каждому из рассмотренных критериев;
- краткое изложение процесса аудита, включая элемент неопределенности и/или проблемы, которые могут отразиться на надежности заключения по результатам аудита;
- подтверждение, что цель аудита соответствия достигнута;
- любые неохваченные вопросы, входящие в область аудита;
- заявление о конфиденциальном характере содержания отчета;
- заключение по результатам аудита.

7.4.7. Отчет по результатам проведения аудита является собственностью Компании.

7.4.8. По завершении внешнего аудита документы, относящиеся к аудиту, должны быть переданы работниками привлеченной организации Компании в установленный договором срок.

7.4.9. Результаты аудита:

- могут служить основанием для инициирования служебного расследования;
- используются для формирования предложений по совершенствованию организационных мер по обеспечению безопасности ПДн и системы защиты ПДн в соответствии с п. 7.1.2. настоящего Положения.

## **8. Порядок действий в случае нештатных ситуаций**

8.1. Под нештатными ситуациями понимается отклонение регламентированного настоящим Положением процесса от запланированного или ожидаемого результата по субъективным либо по не зависящим от участников процесса причинам, которое может привести к неблагоприятным последствиям для Компании или субъектов, ПДн которых обрабатываются Компанией, и требует оперативного вмешательства.

8.2. Работник Компании, столкнувшийся с нештатной ситуацией, обязан незамедлительно сообщить лицу, ответственному за организацию обработки ПДн, следующую информацию:

- общее описание нештатной ситуации;
- сведения о категории субъектов (конкретном субъекте) ПДн, которые могут быть затронуты возникшей нештатной ситуацией;

- текст сообщения об ошибке (если применимо);
- контактные данные исполнителей, уполномоченных участвовать в реагировании на нештатную ситуацию.

8.3. Лицо, ответственное за организацию обработки ПДн, принимает решение о необходимости привлечения к реагированию на нештатную ситуацию работников других структурных подразделений Компании, докладывает об этом Генеральному директору Компании, который назначает оперативное совещание.

8.4. Участники оперативного совещания должны;

- определить условия возникновения нештатной ситуации;
- определить перечень первоочередных мер по минимизации риска возникновения неблагоприятных последствий либо их устранения, установить сроки их выполнения и ответственных работников;
- определить, какие сведения о нештатной ситуации должны быть доведены до работников Компании и третьих лиц.

8.5. Результаты реагирования на нештатную ситуацию:

- могут служить основанием для инициирования служебного расследования;
- используются для формирования предложений по совершенствованию организационных мер по обеспечению безопасности ПДн и системы защиты ПДн в соответствии с п. 7.1.2. настоящего Положения.

## 9. Ответственность за нарушение требований Положения

9.1. Лица, виновные в нарушении требований законодательства Российской Федерации о ПДн, настоящего Положения и иных локальных актов Компании, определяющих порядок обработки и защиты ПДн, несут гражданскую, уголовную, административную, материальную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

9.2. Работники, которые в силу служебных обязанностей имеют доступ к ПДн, несут персональную ответственность за обеспечение выполнения требований по обеспечению их безопасности.

## 10. Порядок пересмотра Положения

10.1. Настоящее Положение подлежит пересмотру в следующих случаях:

- изменение законодательства Российской Федерации о ПДн;
- вынесение уполномоченным органом по защите прав субъектов ПДн предписания об устранении выявленных нарушений требований законодательства Российской Федерации о ПДн, затрагивающих область действия настоящего Положения.

Также корректировка Положения может осуществляться:

- по результатам проведенного контроля выполнения требований законодательства Российской Федерации о ПДн и настоящего Положения;
- по результатам расследования инцидентов нарушения требований законодательства Российской Федерации о ПДн и настоящего Положения;
- по результатам расследования нештатных ситуаций.

## Приложение 1. Инструкция пользователя информационной системы персональных данных.

1. Работник Компании, в должностные обязанности которого входит обработка ПДн, обязан:
  - 1.1. Знать и соблюдать требования законодательства Российской Федерации в области ПДн, локальных актов Компании, регламентирующих вопросы обработки и защиты ПДн.
  - 1.2. Знать требования внутренних нормативных документов Компании, регламентирующих правила обеспечения безопасности информации при работе с программными и техническими средствами информационных систем ПДн.
  - 1.3. Обеспечивать конфиденциальность ПДн, ставших ему известными в связи с выполнением должностных обязанностей.
  - 1.4. Не использовать ПДн, ставшие известными в связи с выполнением должностных обязанностей, в публикациях, открытых документах, выступлениях, переписке, рекламных материалах, презентациях, выставочных проспектах и информационных сообщениях.
  - 1.5. Не распространять работникам Компании или третьим лицам сведения о составе обрабатываемых Компанией ПДн, носителях ПДн, хранилищах ПДн, информационных системах ПДн и способах защиты ПДн.
  - 1.6. Не передавать ПДн по каналам телефонной и факсимильной связи, с использованием сетей Интернет или Интранет без применения мер защиты, согласованных с лицом, ответственным за организацию обработки ПДн.
  - 1.7. Не вести переговоры с передачей ПДн по телефону или в неслужебных помещениях, а также в присутствии посторонних лиц.
  - 1.8. Сообщать лицу, ответственному за организацию обработки ПДн, ставшие известными факты нарушения порядка обработки ПДн.
  - 1.9. В случае возникновения нештатных ситуаций незамедлительно сообщить о них лицу, ответственному за организацию обработки ПДн.
2. Работник Компании обязан соблюдать следующие требования при обращении с материальными носителями ПДн:
  - 2.1. Хранить материальные носители только в установленных хранилищах ПДн.
  - 2.2. Хранить ПДн только на учтенных машинных материальных носителях ПДн.
  - 2.3. Не хранить на одном материальном носителе ПДн, обрабатываемые в разных целях.
  - 2.4. Не хранить материальные носители, содержащие ПДн, обрабатываемые в разных целях, в одном хранилище ПДн.
  - 2.5. Своевременно осуществлять уничтожение материальных носителей ПДн.
  - 2.6. Не выносить материальные носители ПДн за пределы помещений Компании без предварительного согласования с руководителем структурного подразделения.
  - 2.7. Изготавливать несанкционированные копии (распечатывать, сканировать, фотографировать, копировать и т.п.) с материальных носителей ПДн.
3. Работник Компании обязан соблюдать следующие правила при использовании средств автоматизации при обработке ПДн:
  - 3.1. Хранить ПДн только в информационных системах ПДн и, при согласовании с лицом, ответственным за организацию обработки ПДн, на сетевых дисках.

- 3.2. Не передавать личные учетные записи и пароли доступа к информационным системам третьим лицам (в том числе работникам Компании).
  - 3.3. Использовать чужие идентификационные данные для доступа к информационным системам ПДн.
  - 3.4. Не вносить изменения в конфигурацию автоматизированного рабочего места.
  - 3.5. Блокировать доступ к автоматизированному рабочему месту при оставлении его без присмотра.
  - 3.6. Использовать предоставленные им информационные ресурсы в неслужебных целях.
4. Нарушение перечисленных выше требований приравнивается к нарушению трудовой дисциплины Компании.

**Приложение 2. Форма Перечня хранилищ носителей персональных данных**

Журнал начат « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Журнал завершен « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность

Должность

\_\_\_\_\_ / ФИО работника /

\_\_\_\_\_ / ФИО работника /

№ п/п	Описание хранилища (сейф, металлический шкаф)	Местонахождение хранилища (номер комнаты)	Категории субъектов, персональные данные которых хранятся в хранилище	Должности работников, которым выдан ключ от шкафа (сейфа)	Примечание
1.					
2.					

### Приложение 3. Форма Журнала учета машинных носителей персональных данных

Журнал начат « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Журнал завершен « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность

Должность

\_\_\_\_\_ / ФИО работника /

\_\_\_\_\_ / ФИО работника /

№ п/п	Дата постановки / снятия с учета	Тип / емкость носителя	Серийный номер	Местоположение носителя	Сведения об уничтожении носителя / стирании информации	ФИО	Подпись



**Приложение 4. Акт о выделении к уничтожению и уничтожении  
бумажных носителей персональных данных, не подлежащих хранению**

№ \_\_\_\_\_

от « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Комиссия в составе:

\_\_\_\_\_

Фамилия И.О., должность, структурное подразделение

\_\_\_\_\_

Фамилия И.О., должность, структурное подразделение

составила настоящий акт о том, что произведено выделение к уничтожению бумажных носителей персональных данных как утративших практическое значение в составе:

№ пп	Заголовок дела (папки) или групповой заголовок дел	Дата дела или крайние даты документов в деле	Количество дел (томов, частей)	Сроки хранения дела (тома, части)	Примечание

Комиссией было произведено уничтожение носителей персональных данных, выделенных к уничтожению.

Итого \_\_\_\_\_ дел уничтожены путём сожжения/дробления//измельчения/иной способ (нужное подчеркнуть)..

Члены комиссии

\_\_\_\_\_

\_\_\_\_\_

## Приложение 5. Форма запроса субъекта персональных данных

Генеральному директору

ООО «Ренессанс Брокер» Фроловичеву В.В.

от \_\_\_\_\_

(ФИО субъекта персональных данных или его представителя)

---

---

(номер основного документа, удостоверяющего личность субъекта или представителя, сведения о дате выдачи указанного документа и выдавшем его органе)

---

(адрес, по которому должен быть отправлен ответ в случае, если ответ не передается субъекту персональных данных лично в руки)

### ЗАЯВЛЕНИЕ

На основании \_\_\_\_\_

(сведения, подтверждающие участие субъекта персональных данных в отношениях с Компанией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Компанией)

прошу \_\_\_\_\_

---

(суть запроса)

« \_\_\_ » \_\_\_\_\_ 20\_\_ г.

(дата обращения)

\_\_\_\_\_  
(подпись) (расшифровка подписи)



## Приложение 7. Типовая форма ответа на запрос субъекта персональных данных

В ответ на Ваш запрос:

- дата получения запроса;
- ФИО субъекта персональных данных или представителя, указанные в запросе;
- данные паспорта или иного документа, удостоверяющего личность в соответствии с законодательством Российской Федерации (серия, номер), дата выдачи документа: (дата выдачи паспорта или иного документа, удостоверяющего личность в соответствии с законодательством Российской Федерации, указанная в запросе)

Общество с ограниченной ответственностью «Ренессанс Брокер», адрес местонахождения: 123317, г. Москва, Пресненская набережная, д. 10 (далее – Компания) сообщает:

По состоянию на (дата ответа) Компания подтверждает факт обработки ПДн (фамилия, имя, отчество субъекта, указанные в запросе) в целях (указать цели обработки<sup>1</sup>) на следующих правовых основаниях: (указать правовые основания<sup>1</sup>).

Компания применяет следующие способы обработки персональных данных: автоматизированная обработка и неавтоматизированная обработка.

Перечень лиц, которым персональные данные субъекта могут быть раскрыты на основании федеральных законов: (привести перечень лиц, которые имеют доступ к ПДн или которым могут быть раскрыты персональные данные на основании договора с Компанией или на основании федерального закона, за исключением работников Компании).

Перечень лиц, осуществляющих обработку персональных данных субъекта на основании поручения Компании: (привести наименование или фамилии, имена, отчества и адреса лиц, осуществляющих обработку персональных данных по поручению Компании, если обработка поручена или будет поручена таким лицам).

Компания в рамках своей деятельности осуществляет обработку следующего перечня персональных данных: (привести перечень обрабатываемых ПДн<sup>1</sup>).

Указанные выше персональные данные были предоставлены (указать источник предоставления ПДн).

Компания осуществляет хранение персональных данных в следующие сроки: (указать сроки обработки<sup>1</sup>).

Права (ФИО субъекта ПДн, указанные в запросе) как субъекта персональных данных определены в главе 3 Федерального закона от 27.07.06 г. № 152-ФЗ «О персональных данных». Компания устанавливает следующие способы обращения субъектов персональных данных в целях осуществления прав, предусмотренных законодательством Российской Федерации:

- путем направления почтового сообщения на адрес места нахождения Компании;
- путем направления электронного сообщения в форме электронного документа, подписанного квалифицированной электронной подписью в соответствии с законодательством Российской Федерации.

---

\* На основании Перечня ПДн, обрабатываемых в ООО «Ренессанс Брокер»

В отношении указанных выше персональных данных осуществлялась или предполагается осуществлять (не осуществлялась и не предполагается осуществлять) трансграничную передачу на территорию следующих стран: (перечислить страны).

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

(дата ответа)

\_\_\_\_\_  
(подпись работника, подготовившего  
ответ и расшифровка)

## Приложение 8. Типовая форма Журнала учета проверок Компании, проводимых органами государственного контроля (надзора), органами муниципального контроля

\_\_\_\_\_ (дата начала ведения журнала)

Общество с ограниченной ответственностью «Ренессанс Брокер», адрес местонахождения: 123317, г. Москва, Пресненская набережная, д. 10

\_\_\_\_\_ (государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: \_\_\_\_\_  
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала учета проверок)

\_\_\_\_\_ (фамилия, имя, отчество Генерального директора Компании)

Подпись: \_\_\_\_\_  
М.П.

### Сведения о проводимых проверках

1.	Дата начала и окончания проверки	
2.	Общее время проведения проверки	
3.	Наименование органа государственного контроля (надзора), наименование органа муниципального контроля	
4.	Дата и номер распоряжения или приказа о проведении проверки	
5.	Цель, задачи и предмет проверки	
6.	Вид проверки (плановая или внеплановая): в отношении плановой проверки: - со ссылкой на ежегодный план проведения проверок; в отношении внеплановой выездной проверки: - с указанием на дату и номер решения прокурора о согласовании проведения проверки (в случае, если такое согласование необходимо)	
7.	Дата и номер акта, составленного по результатам проверки, дата его вручения представителю юридического лица, индивидуальному предпринимателю	

8.	Выявленные нарушения обязательных требований (указываются содержание выявленного нарушения со ссылкой на положение нормативного правового акта, которым установлено нарушенное требование, допустившее его лицо)	
9.	Дата, номер и содержание выданного предписания об устранении выявленных нарушений	
10.	Фамилия, имя, отчество (в случае, если имеется), должность должностного лица (должностных лиц), проводящего(их) проверку	
11.	Фамилия, имя, отчество (в случае, если имеется), должности экспертов, представителей экспертных организаций, привлеченных к проведению проверки	
12.	Подпись должностного лица (лиц), проводившего проверку	