Утверждено Приказом
Генерального директора
Общества с ограниченной ответственностью «Кредитэкспресс Финанс»
№ 9-П от 19 января 2017 г.

Падош Б. _____

ПОЛОЖЕНИЕО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

«КРЕДИТЭКСПРЕСС ФИНАНС»

(новая редакция)

2017

Настоящее Положение о защите персональных данных (далее — Положение) регулирует отношения по защите персональных данных работников Общества с ограниченной ответственностью «Кредитэкспресс Финанс» (далее — работники), а также лиц, в отношении персональных данных которых Обществом с ограниченной ответственностью «Кредитэкспресс Финанс» (ООО «КЭФ») (далее — Общество) осуществляется обработка в целях исполнения ими договоров, одной из сторон которых они являются (должников), иных лиц.

Настоящее Положение разработано в соответствии с требованиями Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных» (далее — ФЗ «О персональных данных»), Трудовым кодексом Российской Федерации, Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных мер по обеспечению безопасности персональных данных при их обработки в информационных системах персональных данных», Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687, в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Настоящее Положение определяет права субъектов персональных данных при обработке их персональных данных, принципы и условия обработки персональных данных, обязанности работников Общества при обработке персональных данных, меры по обеспечению безопасности персональных данных при их обработке и ответственность за нарушение настоящего Положения.

1. Защита персональных данных лиц, в отношении которых осуществляется обработка с целью исполнения ими договоров, одной из сторон которых они являются (должников), иных лиц

1.1. Понятие персональных данных. Обработка персональных данных и иные основные понятия, используемые в настоящем Положении

1) персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

2) оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В целях исполнения настоящего Положения под оператором понимается Общество;

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

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

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

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

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

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

10) информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

12) субъект персональных данных — физическое лицо, в отношении информации которого Общество осуществляет обработку (работник, должник, иное лицо);

13) должник — лицо, в отношении которого осуществляется взыскание с целью исполнения договора, одной из сторон которого он является.

1.2. Принципы и условия обработки персональных данных

1.2.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

1.2.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

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

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

1.2.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Общество должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

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

1.2.8. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных ФЗ «О персональных данных». Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Общество функций, полномочий и обязанностей;

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

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

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

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в п. 1.3.1.9 настоящего Положения, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных);

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

1.2.9. Общество в своей деятельности осуществляет обработку персональных данных должников исключительно в целях исполнения ими договоров, одной из сторон которых они являются, обеспечивая конфиденциальность таких данных. Обработка персональных данных иных лиц осуществляется в целях, указанных в согласии на обработку персональных данных таких лиц (примерная форма Согласия иных лиц приведена в Приложении № 1.1 к настоящему Положению; примерная форма Согласия на обработку персональных данных соискателей на вакантные должности в Обществе приведена в Приложении № 1.2).

1.2.10. Общество обязано не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено ФЗ «О персональных данных».

1.2.11. Срок обработки персональных данных должников, иных лиц, в том числе срок их хранения определяется в согласии указанных лиц в случаях, когда такое согласие в соответствии с законодательством Российской Федерации необходимо для обработки персональных данных таких лиц.

1.3. Права субъекта персональных данных

1.3.1. Право субъекта персональных данных на доступ к его персональным данным

1.3.1.1. Субъект персональных данных имеет право на получение сведений, указанных в п.

1.3.1.7 настоящего Положения, за исключением случаев, предусмотренных п. 1.3.1.8 настоящего Положения. Субъект персональных данных вправе требовать от Общества уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.3.1.2. Сведения, указанные в п. 1.3.1.7 настоящего Положения, должны быть предоставлены субъекту персональных данных Обществом в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

1.3.1.3. Сведения, указанные в п. 1.3.1.7 настоящего Положения, предоставляются субъекту персональных данных или его представителю Обществом при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Общества, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Работникам Общества запрещается предоставлять персональные данные субъектов персональных данных иным лицам по телефону, факсу, почте без наличия надлежаще оформленного запроса.

1.3.1.4. В случае, если сведения, указанные в п. 1.3.1.7 настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Обществу или направить ему повторный запрос в целях получения сведений, указанных в п. 1.3.1.7 настоящего Положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

1.3.1.5. Субъект персональных данных вправе обратиться повторно к Обществу или направить ему повторный запрос в целях получения сведений, указанных в п. 1.3.1.7 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 1.3.1.4 настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 1.3.1.3 настоящего Положения и, должен содержать обоснование направления повторного запроса.

1.3.1.6. Общество вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным п.п. 1.3.1.4 и 1.3.1.5 настоящего Положения. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Обществе.

1.3.1.7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных Обществом;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Обществом способы обработки персональных данных;

4) наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

1.3.1.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено, если предоставление персональных данных нарушает конституционные права и свободы других лиц, а также в иных случаях, предусмотренных законодательством Российской Федерации.

1.3.1.9. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если Общество не докажет, что такое согласие было получено.

1.3.1.10. Общество обязано немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в п. 1.3.1.9 настоящего Положения.

1.3.2. Право на обжалование действий или бездействия Общества как оператора.

1.3.2.1. Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований законодательства Российской Федерации или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

1.3.2.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1.4. Обязанности Общества

1.4.1. Обязанности Общества при сборе персональных данных

1.4.1.1. При сборе персональных данных Общество (его работники) обязано предоставить субъекту персональных данных по его просьбе информацию, предусмотренную 1.3.1.7 настоящего Положения.

1.4.1.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом (в частности, ч. 3 ст. 14 ФЗ «О персональных данных» — требования к запросу о предоставлении персональных данных), Общество (его работники) обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

1.4.1.3. Если персональные данные получены не от субъекта персональных данных, Общество, за исключением случаев, предусмотренных п. 1.4.1.4 настоящего Положения, до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес Общества или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные ФЗ «О персональных данных» права субъекта персональных данных;

5) источник получения персональных данных.

1.4.1.4. Общество освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 1.4.1.3 настоящего Положения, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных Обществом;

2) персональные данные получены Обществом на основании законодательства Российской Федерации или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) Общество осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных п. 1.4.1.3 настоящего Положения, нарушает права и законные интересы третьих лиц.

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить 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, установленных законодательством Российской Федерации.

1.4.2. Обязанности Общества по обеспечению безопасности персональных данных при их обработке

1.4.2.1. Общество (его работники) при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

1.4.2.2. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

1.4.3. Обязанности Общества при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

1.4.3.1. Общество обязано сообщить в порядке, предусмотренном п. 1.3.1 настоящего Положения субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

1.4.3.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Общество дает в письменной форме мотивированный ответ, содержащий правовое обоснование, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

1.4.3.3. Общество обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Общество обязано внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Общество обязано уничтожить такие персональные данные. Общество уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и должно принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

1.4.3.4. Общество сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

1.4.4. Обязанности Общества по устранению нарушений законодательства, допущенных при обработке персональных данных по уточнению, блокированию и уничтожению персональных данных.

1.4.4.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных, Общество осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или должно обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Общество обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

1.4.4.2. В случае подтверждения факта неточности персональных данных Общество на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо должно обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

1.4.4.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Обществом или лицом, действующим по поручению Общества, Общество в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Общества. В случае, если обеспечить правомерность обработки персональных данных невозможно, Общество в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Общество обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

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

1.4.4.5. Уничтожение персональных данных должников, иных лиц осуществляется способом, исключающим возможность их последующего восстановления и использования (в частности, использование уничтожителей бумаги).

1.4.4.6. В каждом случае уничтожения или блокирования персональных данных должников, иных лиц составляется соответствующий акт. Акт составляется комиссией в составе не менее 3 человек из числа работников Департамента досудебного взыскания, Департамента информационных технологий во главе с председателем — Директором Департамента досудебного взыскания, подписывается и скрепляется фирменной печатью Общества (Приложения №№ 4 и 5).

1.4.4.7. Ответственность за обеспечение сохранности персональных данных должников, иных лиц в процессе их обработки несут руководители Департаментов досудебного взыскания и информационных технологий, генеральный директор Общества.

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

1.4.4.9. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п.п. 1.4.4.3, 1.4.4.4 и 1.4.4.8 настоящего Положения, Общество осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен законодательством Российской Федерации.

.5. Меры по обеспечению безопасности персональных данных при их обработке

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

- назначение ответственного за организацию обработки персональных данных;

- издание документов, определяющих политику Общества в отношении обработки

персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

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

- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;

- ознакомление работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных, формирование на их основе модели угроз;

- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных

применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учет машинных носителей персональных данных;

- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение сохранности носителей персональных данных;

- утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- назначение должностного лица (работник), ответственного за обеспечение безопасности персональных данных в информационной системе.

- предоставление доступа к содержанию электронного журнала сообщений исключительно для сотрудников Оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

- идентификация и аутентификация пользователей, являющихся сотрудниками Оператора;

- идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных;

- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

защита обратной связи при вводе аутентификационной информации;

- идентификация и аутентификация пользователей, не являющихся сотрудниками Оператора (внешних пользователей);

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

- реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;

- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

- ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);

- блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

- регламентация и контроль использования в информационной системе технологий беспроводного доступа;

- регламентация и контроль использования в информационной системе мобильных технических средств;

-управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);

- обеспечение доверенной загрузки средств вычислительной техники;

- управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения;

- управление доступом к машинным носителям персональных данных;

- уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания;

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;

- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

- защита информации о событиях безопасности;

- реализация антивирусной защиты;

- обновление базы данных признаков вредоносных компьютерных программ (вирусов);

- обнаружение вторжений;

- обновление базы решающих правил;

- выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;

- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

- контроль состава технических средств, программного обеспечения и средств защиты информации;

- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе;

- контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;

- обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама);

- периодическое резервное копирование персональных данных на резервные машинные носители персональных данных;

- обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала;

- идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;

- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

- регистрация событий безопасности в виртуальной инфраструктуре;

- управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

- контроль целостности виртуальной инфраструктуры и ее конфигураций;

- резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;

- реализация и управление антивирусной защитой в виртуальной инфраструктуре;

- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей;

- контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

- разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы;

- обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;

- защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных;

- разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы;

- защита беспроводных соединений, применяемых в информационной системе;

- определение лиц, ответственных за выявление инцидентов и реагирование на них;

- обнаружение, идентификация и регистрация инцидентов;

- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

- принятие мер по устранению последствий инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов;

- определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;

- управление изменениями конфигурации информационной системы и системы защиты персональных данных;

- анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных;

- документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных;

-проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

- тестирование информационной системы на проникновения;

- использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования;

- применение средств вычислительной техники не ниже 5 класса;

- применение системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

- применение межсетевых экранов не ниже 3 класса;

- применение средств защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

1.5.2. Для целей настоящего раздела под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Защита персональных данных работников

2.1. Общие требования при обработке персональных данных работника и гарантии их защиты

В целях обеспечения прав и свобод человека и гражданина Общество при обработке персональных данных работника гарантируют соблюдение следующих общих требований:

1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника Общество будет руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами;

3) все персональные данные работника могут быть получены у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Общество сообщает работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) Общество не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и другими федеральными законами;

5) Общество не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом или иными федеральными законами;

6) при принятии решений, затрагивающих интересы работника, Общество не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты обеспечивается Обществом за счет его средств в порядке, установленном Трудовым кодексом и иными федеральными законами;

8) работники и их представители должны быть ознакомлены под роспись с документами Общества, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) Общество, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

.2. Хранение и использование персональных данных работников

2.2.1. Персональные данные работников хранятся в местах, исключающих возможность их несанкционированного использования (персональные данные работника на бумажных, магнитных, магнитно-оптических и иных носителях — в железных несгораемых шкафах, запираемых на ключ; персональные данные работника в электронной форме — в файлах с ограниченным правом доступа к ним) лицами, не уполномоченными на то Обществом.

2.2.2. Персональные данные каждого работника хранятся отдельно от персональных данных других работников.

2.2.3. Правом доступа к персональным данным работников обладают наравне с работником лица, имеющие в силу должностного положения отношение к их использованию (работники Департамента по работе с персоналом, Департамента финансов, Юридического департамента) и только в случаях служебной еобходимости.

Использование персональных данных работника иными лицами и в иных целях не допускается.

Передача персональных данных работника в пределах Общества осуществляется лицами из числа работников Департаментов, указанных в абз. 1 настоящего пункта, в любой форме (устной, письменной), с использованием при необходимости почтовой, телефонной, телетайпной, факсимильной, электронной и иной связи. При передаче персональных данных работника должны быть предприняты все необходимые меры для исключения возможности их разглашения.

2.2.4. Для обеспечения защиты персональных данных других работников, а также персональных данных должников и иных лиц, работники перед началом исполнения своих должностных обязанностей дают расписку о неразглашении информации, содержащей персональные данные (Приложение № 2).

2.2.5. Работник Общества при прекращении трудовых отношений с Обществом обязан в последний день работы передать Обществу имеющиеся в его пользовании материальные носители информации, содержащие персональные данные других работников Общества, должников, иных лиц.

2.2.6. Персональные данные работников подлежат хранению не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами.

Срок обработки персональных данных работников, в том числе срок их хранения составляет 75 лет, если иной срок не определен в Согласии на обработку персональных данных работника (Приложение № 1).

2.2.7. О прекращении обработки персональных данных работника и их уничтожении Общество уведомляет работника или его представителя. Уведомление осуществляется в форме, позволяющей установить факт его направления и получения адресатом.

2.2.8. Уничтожение персональных данных работника осуществляется способом, исключающим возможность их последующего восстановления и использования (в частности, использование уничтожителей бумаги).

2.2.9. В каждом случае уничтожения или блокирования персональных данных работника составляется соответствующий акт. Акт составляется комиссией в составе не менее 3 человек из числа работников Департамента финансов и Юридического департамента во главе с председателем — руководителем Департамента по работе с персоналом, подписывается и скрепляется фирменной печатью Общества (Приложения №№ 4 и 5).

2.2.10. Ответственность за обеспечение сохранности персональных данных работника в процессе их хранения и использования, в том числе передачи несут руководитель Департамента по работе с персоналом, финансовый директор.

2.3. Передача персональных данных работника

При передаче персональных данных работника Общество гарантирует ему, что:

не будет сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами;не будет сообщать персональные данные работника в коммерческих целях без его письменного согласия; предупредит лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и будет требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности).

Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым кодексом и иными федеральными законами;

будет осуществлять передачу персональных данных работника в пределах Общества в соответствии с настоящим Положением, с которым работник должен быть ознакомлен под роспись (Приложение № 3);

будет разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица будут иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

не будет запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

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

2.4. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

В целях обеспечения защиты персональных данных, хранящихся в Обществе, работники имеют право на:

полную информацию об их персональных данных и обработке этих данных;

свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

определение своих представителей для защиты своих персональных данных;

доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса или иного федерального закона. При отказе Общества исключить или исправить персональные данные работника он имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

требование об извещении Обществом всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжалование в суд любых неправомерных действий или бездействия Общества при обработке и защите его персональных данных.

3. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

3.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее — персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

3.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее — материальные носители), в специальных разделах или на полях форм (бланков).

3.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Фиксация на одном материальном носителе персональных данных работников, должников, иных лиц не допускается.

3.4. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Общества или лица, осуществляющие такую обработку по договору с Обществом), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Обществом без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Общества.

3.5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее — типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Общества, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, — при необходимости получения письменного согласия на обработку персональных данных;

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

3.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

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

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

3.8. Правила, предусмотренные п.п. 3.6 и 3.7 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

3.9. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3.10. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.11. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

Материальные носители персональных данных работников, должников, иных лиц хранятся отдельно друг от друга.

4. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.