Приложение № 2
к Политике по обработке и защите персональных данных
в Банке «ИТУРУП» (ООО)

Публичная политика по обработке и защите персональных данных

1. Общие положения

1.1.Настоящая Публичная политика по обработке и защите персональных данных отражает основные подходы, политику Банка «ИТУРУП» (ООО) (далее – Банк) в отношении обработки и защиты персональных данных, содержит сведения о реализуемых требованиях к защите персональных данных.

1.2.Настоящая Публичная политика по обработке и защите персональных данных (далее – Публичная политика) разработана в целях обеспечения защиты прав и свобод клиентов Банка, представителей клиентов Банка, выгодоприобретателей, бенефициарных владельцев клиентов Банка, работников Банка и иных субъектов персональных данных (далее – субъект персональных данных) при обработке Банком их персональных данных. Публичная политика подлежит опубликованию на официальном веб-сайте Банка в сети «Интернет» либо размещению на информационном стенде в отделениях Банка с предоставлением к нему неограниченного доступа любым заинтересованным лицам.

1.3.Публичная политика разработана в соответствии с Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 года 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Федеральным законом от 07.08.2001 года N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», иными федеральными законами, Постановлением Правительства Российской Федерации от 15.09.2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.11.2012 года N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными актами, в том числе внутренними документами Банка «ИТУРУП» (ООО) (далее – Банк), стандартами Банка России в области информационной безопасности и защиты персональных данных.

2. Принципы обработки персональных данных

При обработке персональных данных Банк руководствуется следующими принципами:

2.1. Обработка персональных данных осуществляется на законной и справедливой основе.

2.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

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

2.5. Содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки.

2.6. При обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Банк принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

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

3. Условия обработки персональных данных

3.1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ, Публичной политикой, внутренними документами Банка. Обработка персональных данных допускается Банком в следующих случаях:

3.1.1. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

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

3.1.3. 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;

3.1.4. обработка персональных данных осуществляется в иных случаях, предусмотренных действующим законодательством, когда получение согласия субъекта персональных данных не требуется.

3.2. Банк и работники Банка, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.3. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Банком.

3.4. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Банк вправе продолжить обработку персональных

данных без согласия субъекта персональных данных при наличии оснований, указанных в п.п. 3.1.2. – 3.1.4. Публичной политики.

3.5. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

3.5.1. фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

3.5.2. фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3.5.3. наименование и адрес Банка;

3.5.4. цель обработки персональных данных;

3.5.5. перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

3.5.6. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка будет поручена такому лицу;

3.5.7. перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Банком способов обработки персональных данных;

3.5.8. срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

3.5.9. подпись субъекта персональных данных.

3.6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

3.7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

3.8. Персональные данные могут быть получены Банком от лица, не являющегося субъектом персональных данных, при условии предоставления Банку подтверждения наличия оснований, указанных в п.п. 3.1.2. – 3.1.4. Публичной политики.

3.9. Банк не обрабатывает персональные данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

Персональные данные, касающиеся состояния здоровья, обрабатываются Банком исключительно в отношении работников Банка строго в соответствии с трудовым законодательством.

4. Права субъекта персональных данных

4.1.Субъект персональных данных имеет право на получение сведений, указанных в п. 4.7. Публичной политики, за исключением случаев, предусмотренных п. 4.8. Публичной политики. Субъект персональных данных вправе требовать от Банка 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.

4.2.Сведения, указанные в п. 4.7. Публичной политики, предоставляются субъекту персональных данных Банком в доступной форме, Банк не раскрывает персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4.3.Сведения, указанные в п. 4.7. Публичной политики, предоставляются субъекту персональных данных или его представителю Банком 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 Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком, 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.

4.4.В случае, если сведения, указанные в п. 4.7. Публичной политики, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Банк или направить ему повторный запрос в целях получения сведений, указанных в п. 4.7. Публичной политики, 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.

4.5.Субъект персональных данных вправе обратиться повторно в Банк или направить ему повторный запрос в целях получения сведений, указанных в п. 4.7. Публичной политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 4.4. Публичной политики, 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. 4.3. Публичной политики, должен содержать обоснование направления повторного запроса.

4.6.Банк вправе мотивированно отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным п. 4.4. и п. 4.5. Публичной политики.

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

4.7.1. подтверждение факта обработки персональных данных Банком;

4.7.2. правовые основания и цели обработки персональных данных;

4.7.3. цели и применяемые Банком способы обработки персональных данных;

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

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

4.7.6. сроки обработки персональных данных, в том числе сроки их хранения;

4.7.7. порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

4.7.8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;

4.7.9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;

4.7.10. иные сведения, предусмотренные федеральными законами.

4.8.Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

4.8.1. обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4.8.2. в иных случаях, предусмотренных Федеральным законом № 152-ФЗ.

4.9.Если субъект персональных данных считает, что Банк осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Банка в уполномоченный орган по защите прав субъектов персональных данных[1] или в судебном порядке.

5. Обязанности Банка

5.1. При сборе персональных данных Банк предоставляет субъекту персональных данных по его просьбе информацию, предусмотренную п. 4.7. Публичной политики.

5.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Банк разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

5.3. Если персональные данные получены не от субъекта персональных данных, Банк, за исключением случаев, предусмотренных п. 5.4. Публичной политики, до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию:

5.3.1. наименование и адрес Банка или его представителя;

5.3.2. цель обработки персональных данных и ее правовое основание;

5.3.3. предполагаемые пользователи персональных данных;

5.3.4. установленные Федеральным законом № 152-ФЗ права субъекта персональных данных;

5.3.5. источник получения персональных данных.

5.4. В соответствии с Федеральным законом № 152-ФЗ Банк освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 5.3. Публичной политики, в случаях, если:

5.4.1. субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором[2];

5.4.2. персональные данные получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

---

[1] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальные органы.

[2] 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.

5.4.3. персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

5.4.4. в иных случаях, предусмотренных Федеральным законом № 152-ФЗ.

5.5. Банк сообщает в порядке, предусмотренном п. 4.1. – п. 4.8. Публичной политики, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет 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.

5.6. 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 Банк дает в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, 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.

5.7. Банк предоставляет 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, Банк вносит 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, Банк уничтожает такие персональные данные. Банк уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

5.8. Банк 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.

5.9. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Банк осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) 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 Банк осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) 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.

5.10. В случае подтверждения факта неточности персональных данных Банк 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 обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

5.11. В случае выявления неправомерной обработки персональных данных, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Банка. В случае, если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Банк уведомляет 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.

5.12. В случае достижения цели обработки персональных данных Банк прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) 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 Банком и субъектом персональных данных либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

5.13. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Банк прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) 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 Банком и субъектом персональных данных либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

5.14. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п. 5.11. – п. 5.13. Публичной политики, Банк осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6. Меры по защите и обеспечению безопасности персональных данных при их обработке в Банке

6.1. Банк принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Политикой по обработке и защите персональных данных в Банке «ИТУРУП» (ООО), Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом № 152-ФЗ или другими федеральными законами. К таким мерам, в частности, относятся:

6.1.1. назначение Банком ответственного за организацию обработки персональных данных;

6.1.2. издание Банком Политики по обработке и защите персональных данных в Банке «ИТУРУП» (ООО);

6.1.3. применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

6.1.4. осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Политике по обработке и защите персональных данных в Банке «ИТУРУП» (ООО), внутренним документам Банка;

6.1.5. оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

6.1.6. ознакомление работников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, Политикой по обработке и защите персональных данных в Банке «ИТУРУП» (ООО), внутренними документами Банка, и (или) обучение указанных работников.

6.2. В Банке назначается лицо, ответственное за организацию обработки персональных данных.

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

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

6.3. Банк при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.4. Обеспечение безопасности персональных данных достигается, в частности:

6.4.1. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

6.4.2. применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных, в том числе:

6.4.2.1. идентификация и аутентификация субъектов доступа и объектов доступа;

6.4.2.2. управление доступом субъектов доступа к объектам доступа;

6.4.2.3. ограничение программной среды;

6.4.2.4. защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

6.4.2.5. регистрация событий безопасности;

6.4.2.6. защита от воздействия вредоносного кода;

6.4.2.7. обнаружение (предотвращение) вторжений;

6.4.2.8. контроль (анализ) защищенности персональных данных;

6.4.2.9. обеспечение доступности персональных данных;

6.4.2.10. защита технических средств;

6.4.2.11. защита информационной системы, ее средств, систем связи и передачи данных;

6.4.2.12. выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных;

6.4.2.13. управление конфигурацией информационной системы и системы защиты персональных данных;

6.4.3. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

6.4.4. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

6.4.5. учетом машинных носителей персональных данных;

6.4.6. обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

6.4.7. восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

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

6.4.9. контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

6.4.10. определением перечня персональных данных, обрабатываемых в Банке;

6.4.11. осуществлением классификации информационных систем персональных данных и определением уровня защищенности персональных данных.

6.5. Использование и хранение биометрических персональных данных вне информационных систем персональных данных осуществляется 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.

6.6. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации

их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

6.7. 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 используется отдельный материальный носитель.

6.8. Лица, осуществляющие обработку персональных данных без использования средств автоматизации информируются о факте обработки ими персональных данных, обработка которых осуществляется Банком 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 Банка.

6.9. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска на территорию, на которой находится Банк, или в иных аналогичных целях, соблюдаются следующие условия:

6.9.1. необходимость ведения такого журнала (реестра, книги) устанавливается внутренним документом Банка, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Банк, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

6.9.2. копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

6.9.3. персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Банк.

6.10. 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, принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

6.10.1. 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;

6.10.2. 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.

6.11. 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).

6.12. Правила, предусмотренные пунктами 6.9 и 6.10 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

6.13. 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.

6.14. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется 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.

6.15. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

6.16. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

6.17. В соответствии с договорами на предоставление охранных услуг в Банке обеспечивается физическая охрана, а также установлена и функционирует пожарно-охранная сигнализация.

6.18. В целях предупреждения и выявления нарушений в области обработки и защиты персональных данных служба внутреннего контроля Банка не реже 1 раза в год проводит плановые проверки соблюдения законодательства о персональных данных в Банке. Служба внутреннего контроля в соответствии с внутренними документами Банка осуществляет также внеплановые проверки.

7. Ответственность за нарушение требований Федерального закона № 152-ФЗ

7.1. Лица, виновные в нарушении требований Федерального закона № 152-ФЗ, несут дисциплинарную, административную, уголовную ответственность, предусмотренную законодательством Российской Федерации.

7.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ, возмещается в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.