УТВЕРЖДЕНО
Правлением АО БАНК «Ермак»
Протокол от «30» 04 2024 г.
Исполняющий обязанности
Председателя Правления
АО БАНК «Ермак»

_____
О. А. Чеботаренко

Публичная политика по обработке и защите персональных данных Акционерного общества Нижневартовский городской банк «Ермак» (АО БАНК «Ермак»)

г. Нижневартовск 2024 год

Содержание

1. Список сокращений

ПДн – Персональные данные
ИСПДн – Информационные системы персональных данных
СЗИ – Система защиты информации
ИБ – Информационная безопасность
НСД – Несанкционированный доступ
ЛВС – Локальная вычислительная сеть
ИС – Информационная система
СИБ – Служба Информационной безопасности
СКУД – Система контроля и управления доступом

2. Общие положения

2.1. Настоящая Публичная политика по обработке и защите персональных данных отражает основные подходы, политику АО БАНК «Ермак» (далее – Публичная политика, Банк) в отношении обработки и защиты персональных данных.

Настоящая 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 ПДн (далее – субъект) при обработке Банком их персональных данных.

2.2. В процессе обработки персональных данных Банк руководствуется следующими основными принципами:

– обработка персональных данных осуществляется на законном и справедливом основании;

– обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

– не допускается обработка персональных данных, несовместимая с целями их обработки;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только персональные данные, которые отвечают целям их обработки, содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки;

– обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки;

– при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;

– неполные или неточные персональные данные уточняются или удаляются;

– 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 уничтожаются по достижении целей их обработки;

– в случае утраты необходимости достижения целей обработки обрабатываемые персональные данные уничтожаются либо обезличиваются.

2.3. Публичная политика разработана в соответствии с:

– Конституцией Российской Федерации;
– Трудовым кодексом Российской Федерации;
– Федеральным законом РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее Закон №152-ФЗ);
– Федеральным законом от 21 июля 1997 г. № 118-ФЗ «Об органах принудительного исполнения Российской Федерации»;
– Федеральным законом от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
– Федеральным законом от 23 декабря 2003 г. № 177-ФЗ «О страховании вкладов в банках Российской Федерации»;

– Федеральным законом от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях»;
– Постановлением Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
– Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
– Приказом ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
– Приказом ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";
– «Специальными требованиями и рекомендации по технической защите конфиденциальной информации (СТР-К)» ФСТЭК России;
– Уставом АО БАНК «Ермак»;
– другие нормативные и правовые документы.

2.4. Требования настоящей Публичной политики обязательны для выполнения всеми Сотрудниками Банка, включая все структурные подразделения, в соответствии с занимаемыми должностями и выполняемыми должностными обязанностям.

Публичная политика является общедоступным документом и предусматривает возможность ознакомления с ней любых лиц путем опубликования в сети Интернет на официальном сайте Банка.

Банк является оператором по обработке персональных данных.

3. Основные понятия

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание: Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

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.

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

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным Законом от 27 июля 2006 г. №152-ФЗ.

Система защиты информационных систем Банка – совокупность программных, аппаратных и технических средств защиты информации, используемых для обеспечения информационной безопасности информационных систем Банка.

Банк — кредитная организация, организующая и (или) осуществляющая обработку персональных данных, а также определяющая цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

Субъект - физическое или юридическое лицо, находящееся на обслуживании в Банке, а также лица, являющиеся в соответствии с законодательством Российской Федерации представителями субъекта, выгодоприобретателями и бенефициарными владельцами.

Сотрудник - физическое лицо, которое вступило в трудовые отношения с Банком.

4. Процесс обработки персональных данных Субъектов Банка

4.1 Обработка персональных данных Субъекта

Персональные данные субъекта могут обрабатываться только с согласия субъекта для целей, непосредственно связанных с деятельностью Банка, в частности, для оказания заявленных банковских услуг, осуществления видов деятельности, указанных в Уставе Банка.

Категории субъектов, ПДн которых обрабатываются в Банке:

- Работники, соискатели, родственники работников, уволенные сотрудники.

  – Цель обработки персональных данных - выполнение трудового законодательства Российской Федерации, исполнения судебных актов, предписаний и требований уполномоченных органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

  для исполнения обязанностей, возложенных на Банк законодательством Российской Федерации;

  – Перечень персональных данных:

  фамилия, имя, отчество, сведения о смене ФИО, гражданство, сведения о работе, ИНН, паспортные данные, данные водительского удостоверения, отношение к военной службе, страховое свидетельство (пентонное), телефон, почтовый адрес, адрес электронной почты, место жительства (регистрации), сведения об образовании, сведения о доходах (расходах), семейное положение, данные о семье, сведения о вкладах и имуществе, дата рождения, место рождения.

- Клиенты банка.
  - Цель обработки персональных данных - заключение и исполнение договоров с контрагентами, представителями которых являются субъекты персональных данных, либо непосредственно с субъектами персональных данных;

    привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок);

    размещение, привлеченных во вклады (до востребования и на определенный срок) денежных средств физических и юридических лиц от имени и за счет Банка;

    открытие и ведение банковских счетов физических и юридических лиц; осуществление расчеты по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам;

    проведение операций, связанных с наличным денежным оборотом по банковскому счету юридического лица и ИП;

    заключение и ведение кредитных договоров, договоров поручительств, договоров залога, доверенностей;

    осуществление переводов денежных средств по поручению физических лиц без открытия банковских счетов (за исключением почтовых переводов);

    оказание других услуг, предусмотренных лицензиями и уставом банка; противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.
  - Перечень персональных данных:

    фамилия, имя, отчество, дата рождения, место рождения, имущественное положение, доходы, адрес электронной почты, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, реквизиты банковской карты, номер расчетного счета, номер лицевого счета.

- Акционеры Банка

  Цель обработки персональных данных - осуществление управленческой деятельности Банка.
  - Перечень персональных данных:

    фамилия, имя, отчество, дата и место рождения, адрес регистрации, паспортные данные, телефон, данные о количестве акций.

Основание для обработки ПДн в Банке зависит от особенностей построения технологического процесса обработки каждой ИСПДн. В Банке ведется автоматизированная и неавтоматизированная обработка ПДн Субъекта.

Сбор, хранение, использование и распространение, в том числе передача третьим лицам ПДн Субъекта без его письменного согласия, Банком запрещены.

Передача ПДн третьим лицам возможна без письменного согласия Субъекта в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законодательством РФ.

В Банке не ведется сбор и обработка ПДн Субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

Сотрудники Банка, в должностные обязанности которых входит обработка ПДн Субъекта, при приеме на работу подписывают «Соглашение о неразглашении персональных данных Клиента» (далее Соглашение). Подписанные Соглашения хранятся в Отделе по работе с персоналом в личном деле каждого сотрудника Банка. Сотрудники, не подписавшие данное Соглашение, к обработке ПДн Субъекта не допускаются.

В Банке осуществляется обработка общей категории персональных данных.

Все ПДн Субъекта, обработка которых ведется в Банке, должны быть получены у него самого, после предоставления им письменного Согласия на обработку переданных им в Банк его персональных данных, с возможностью передачи третьим лицам, должны соответствовать требованиям Закона №152-ФЗ и содержать следующие сведения:

– фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

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

– наименование или фамилию, имя, отчество и адрес Банка, получающего согласие субъекта персональных данных;

– цель обработки ПДн;

– перечень ПДн, на обработку которых дается согласие Субъекта ПДн;

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

– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Банком способов обработки ПДн;

– срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись субъекта ПДн.

В Согласии также указано, что все сообщенные Субъектом ПДн, Банк может обрабатывать, в т.ч. хранить, в любой форме, при этом субъект персональных данных соглашается с условиями обработки, хранения, способов защиты его ПДн и с тем, что Банк имеет право на передачу его персональных данных третьим лицам на основании требований законодательства РФ и требований бизнес-процессов Банка.

Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.

Согласно статье 6 части 1 пункта 5 Федерального Закона №152-ФЗ обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем 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. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

4.2 Права и обязанности Субъекта

Субъект Банка при обработке его ПДн в Банке, как субъект персональных данных, имеет право на получение информации касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Банком;

– правовые основания и цели обработки персональных данных;

– цели и применяемые Банком способы обработки персональных данных;

– 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;

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

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Законом №152-ФЗ;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

Субъект имеет право:

– на доступ к информации о самом себе;

– на определение форм и способов обработки ПДн;

– на отзыв согласия на обработку ПДн;

– ограничивать способы и формы обработки персональных данных;

– устанавливать запрет на распространение ПДн без его согласия;

– требовать изменение, уточнение, уничтожение информации о самом себе;

– обжаловать неправомерные действия или бездействия по обработке ПДн и требовать соответствующей компенсации в суде;

– на дополнение ПДн оценочного характера заявлением, выражающим его собственную точку зрения;

– определять представителей для защиты своих ПДн;

– требовать от Банка уведомления всех лиц, которым ранее были сообщены неверные или неполные ПДн Субъекта, обо всех произведенных в них изменениях или исключениях из них.

Для предоставления вышеперечисленной информации Субъект оформляет Заявление на предоставление информации, связанной с обработкой ПДн в Банке. Оформленное Заявление предоставляется Сотруднику, осуществляющему сбор ПДн Субъекта, который передает Заявление ответственному Сотруднику Службы информационной безопасности (Начальнику службы информационной безопасности или лицу, его замещающему). Ответственный Сотрудник готовит запрашиваемую Субъектом информацию в срок в течение 10 рабочих дней с момента обращения либо получения заявления и передает Сотруднику, выполняющему сбор ПДн, который в дальнейшем предоставляет ее Субъекту для ознакомления. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Сведения о наличии персональных данных должны быть предоставлены Субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Право Субъекта на доступ к своим ПДн ограничивается в случае, если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также, если предоставление ПДн нарушает конституционные права и свободы других лиц.

4.3 Передача персональных данных Субъекта третьим лицам

При передаче ПДн Субъекта Банка третьим лицам соблюдаются следующие требования:

– не сообщать ПДн Субъекта третьим лицам без его письменного согласия, за исключением случаев, предусмотренных законодательством РФ;

– предупредить лиц, получающих ПДн Субъекта о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн Субъекта, обязаны соблюдать режим конфиденциальности;

– накладывать обязательства по защите ПДн Субъекта, которые должны быть установлены в договоре;

– субъект вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений пункта 4.3 настоящей Публичной политики или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

Данные требования не применяются в случае обработки персональных данных в целях выполнения, возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.

Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.4 Ответственность

Каждый Сотрудник Банка, осуществляющий обработку ПДн Субъекта, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн Субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

Неправомерность деятельности Банка по сбору и использованию ПДн Субъекта может быть установлена в судебном порядке.

5. Автоматизированная обработка персональных данных в АО БАНК «Ермак»

Автоматизированная обработка ПДн в Банке осуществляется в рамках ИСПДн, представленных в «Перечне информационных систем АО БАНК «Ермак»». При этом для каждой из ИСПДн документально определены:

– уровень защищенности ИСПДн;
– состав обрабатываемых ПДн;
– категория обрабатываемых ПДн;
– режим обработки ПДн;
– количество субъектов ПДн;
– основание для обработки ПДн;
– состав программно-технических (аппаратных, программных и аппаратно-программных) средств ИСПДн;
– структурная схема ИСПДн;
– схема информационных потоков ИСПДн и роли;
– процесс обработки ПДн.

Для каждой ИСПДн должны быть выполнены требования системы обеспечения информационной безопасности Банка, сформированные на основании требований Законодательства РФ и нормативных актов Регуляторов ФСБ, ФСТЭК, Роскомнадзора и Банка России.

В связи с тем, что персональные данные чаще всего обрабатываются в совокупности с другими категориями защищаемой информации, например, банковской тайной, ко всем информационным системам Банка, перечисленным в «Перечне информационных систем АО БАНК «Ермак»», в том числе и к ИСПДн, предъявляются общие требования по обеспечению информационной безопасности, если иное не установлено внутренними нормативными документами Банка. Данные требования отражаются в Корпоративной политике ИБ Банка и соответствующих Частных политиках.

Используемые технические средства защиты в случае требований нормативных документов должны иметь сертификат соответствия ФСТЭК и ФСБ России на использование в ИСПДн, в соответствии с Моделью угроз и нарушителя ИБ и уровнем защищенности ИСПДн, определенным в «Перечне информационных систем АО БАНК «Ермак», подлежащих защите».

5.1 Процесс автоматизированной обработки персональных данных

Сбор ПДн, занесение данных в ИСПДн и дальнейшая деятельность по обработке и удалению ПДн проводится Сотрудниками (пользователями ИСПДн), ответственными за выполнение вверенных ему операций, в рамках своих должностных обязанностей. При этом круг должностей пользователей, эксплуатирующих программно-технические средства ИСПДн в процессе выполнения своих служебных обязанностей, документально определен Перечнем должностей Банка допущенных к обработке ПДн, согласованным с Начальником Службы информационной безопасности и утвержденным распорядительным документом Председателя Правления Банка. В случае изменения в структуре подразделений и должностей Банка данный перечень пересматривается и утверждается распорядительным документом Председателя Правления Банка. Обязанности по сопровождению ИСПДн возложены на администратора ИСПДн, который назначается соответствующим распорядительным документом Председателя Правления из числа Сотрудников Отдела информационных технологий и технического сопровождения и Отдела Сопровождения программного обеспечения.

Обязанности по обеспечению ИБ ИСПДн возложены на администратора информационной безопасности, который назначается соответствующим распорядительным документом Председателя Правления из числа Сотрудников Службы информационной безопасности.

Пользователям ИСПДн Банка предоставляется право работать только с теми средствами и информационными ресурсами ИСПДн, которые необходимы им для выполнения своих установленных должностных обязанностей.

К автоматизированной обработке ПДн при помощи ИСПДн допускаются Сотрудники Банка, подписавшие «Соглашение о неразглашении персональных данных Клиента» и/или подписавшие «Соглашение о неразглашении персональных данных Сотрудника».

Ответственность за обеспечение защиты информации в процессе эксплуатации средств вычислительной техники, предназначенных для обработки ПДн, возлагается на пользователей, производящих ее обработку.

Любое лицо из числа пользователей ИСПДн Банка должно сообщать о ставшем ему известном факте нарушения или обхода системы защиты информации (далее СЗИ) администратору информационной безопасности ИСПДн и своему непосредственному руководителю.

Доступ к программно-техническим средствам ИСПДн Банка является персонифицированным: каждый пользователь должен иметь и предъявлять при обращении

к программно-техническим средствам ИСПДн Банка атрибуты безопасности, включающие уникальный идентификатор пользователя, пароль (пароли) и (или) аутентифицирующую информацию. Атрибуты безопасности пользователя должны сохраняться им в тайне от посторонних лиц.

5.2 Требования к организации автоматизированной обработки персональных данных

Сопровождение СЗИ на стадии эксплуатации ИСПДн Банка, включая ведение служебной информации средств защиты от НСД (генерацию и смену паролей и ключей пользователей), оперативный контроль за функционированием системы защиты информации, контроль соответствия общесистемной программной среды эталону (контроль целостности программного обеспечения), настройку программных и программно-технических средств, создание замкнутой программной среды, а также контроль за ходом технологического процесса обработки информации путем регистрации и анализа действий пользователей по системному журналу, осуществляется администратором информационной безопасности ИСПДн.

Настройка средств из состава системы защиты информации ИСПДн Банка осуществляется администратором информационной безопасности или системным администратором под контролем администратора информационной безопасности ИСПДн в соответствии с эксплуатационной документацией на средства из состава СЗИ ИСПДн.

В обязанности администратора информационной безопасности входит учет, хранение и выдача пользователям персональных идентификаторов, съемных носителей информации, паролей и ключей для средств защиты информации от НСД.

При эксплуатации ИСПДн, к настройке и конфигурированию средств защиты информации из состава СЗИ ИСПДн Банка должен быть допущен только администратор информационной безопасности или системный администратор под контролем администратора информационной безопасности ИСПДн. Какие-либо другие лица к данным работам не допускаются.

В процессе обеспечения информационной безопасности ИСПДн соблюдаются требования следующих документов, предъявляемые к защищаемой информации:

- «Положение об обеспечении информационной безопасности при управлении доступом и регистрацией к ИС АО БАНК «Ермак»;
- «Частной политики по использованию средств криптографической защиты информации в АО БАНК «Ермак»;
- «Частной политики по обеспечению антивирусной защиты в АО БАНК «Ермак»;
- «Частной политики по использованию корпоративной ЛВС в АО БАНК «Ермак»;
- «Частной политики по использованию ресурсов сети Интернет и электронной почты в АО БАНК «Ермак»;
- «Частной политики парольной защиты в АО БАНК «Ермак»;
- «Частной политики резервного копирования и восстановления данных в АО БАНК «Ермак»;
- «Частной политики по внесению изменений в информационные системы АО БАНК «Ермак» в области ИБ»;
- «Частной политики по обеспечению информационной безопасности при работе с персоналом в АО БАНК «Ермак»;
- «Частной политики по обеспечению информационной безопасности банковских платежных технологических процессов в АО БАНК «Ермак»;
- Руководства администратора ИБ АО БАНК «Ермак»;
- Руководства пользователя ИС АО БАНК «Ермак» по ИБ;
- Руководства по эксплуатации СИБ АО БАНК «Ермак».

Программно-технические средства из состава ИСПДн АО БАНК «Ермак» размещены в помещениях, расположенных в пределах контролируемой зоны Банка. Носители персональных данных определены и учтены.

Помещения, в которых допускается размещение программно-технических средств ИСПДн АО БАНК «Ермак», отвечают требованиям пожарной и электробезопасности, надежно охраняются и имеют:

– прочные двери, оборудованные надежными запорами или кодовыми замками, а также приспособлениями для опечатывания или СКУД;

– сигнализацию, связанную с подразделением охраны или дежурным по подразделению.

Серверные комнаты, с устанавливаемыми в них телекоммуникационным оборудованием (серверами и средствами их управления, телекоммуникационным оборудованием), также должны удовлетворять вышеперечисленным требованиям, при этом доступ в данные помещения должен иметь администратор информационной безопасности ИСПДн и системный администратор ИСПДн.

Каналы связи (между компонентами ИСПДн АО БАНК «Ермак»), расположенные в пределах контролируемой зоны, должны прокладываться в кабель-каналах, препятствующих осуществлению несанкционированного к ним подключения.

Вход в помещения, в которых производится автоматизированная обработка ИСПДн, разрешается постоянно работающим в них пользователям ИСПДн Банка (Перечень должностных лиц, допущенных к обработке персональных данных).

По окончании рабочего дня все помещения, в которых размещены программно-технические средства ИСПДн Банка, запираются, доступ контролируется системами видеонаблюдения и системой контроля и управления доступом.

Корпуса используемых в ИСПДн Банка программно-технических средств, опечатываются таким образом, чтобы исключить их несанкционированное вскрытие (например, специальными саморазрушающимися наклейками или пломбами). Администратор информационной безопасности ИСПДн должен осуществлять периодическую проверку целостности данных средств.

Регламентное обслуживание или устранение неисправности программно-технических средств из состава средств автоматизации ИСПДн Банка, проведение которого повлечет вскрытие данных средств с нарушением целостности специальных защитных средств, осуществляется в присутствии администратора информационной безопасности ИСПДн.

Установка программного обеспечения ИСПДн Банка проводится системным администратором ИСПДн, под контролем администратора информационной безопасности ИСПДн. Дистрибутивы устанавливаемого программного обеспечения должны предварительно проверяться.

Требования к уничтожению информации с носителей и самих носителей ПДн определяются порядком удаления информации и уничтожения носителей согласно «Руководству по эксплуатации системы информационной безопасности АО БАНК «Ермак»».

Ответственность за уничтожение информации с носителей возлагается на пользователя ИСПДн, за уничтожение носителей информации – на администратора ИБ.

6. Неавтоматизированная обработка персональных данных в АО БАНК «Ермак»

В рамках банковских технологических и информационных процессов ведется неавтоматизированная обработка ПДн. Неавтоматизированная обработка ПДн в АО БАНК «Ермак» является вспомогательной деятельностью при организации процесса обработки ПДн в рамках ИСПДн.

Неавтоматизированная обработка ПДн в Банке заключается в работе с бумажными носителями информации, которые содержат сведения, составляющие ПДн (далее – бумажные носители ПДн). К бумажным носителям ПДн Банка в частности относятся:

– Анкеты, заявления, письма, договоры и иные документы на бумажных носителях, получаемые от Субъектов Банка содержащие ПДн;

– Анкеты, заявления, договоры и иные документы на бумажных носителях, получаемые от Сотрудников Банка содержащие ПДн.

6.1 Процесс неавтоматизированной обработки персональных данных

В Банке установлены следующие требования к хранению бумажных носителей ПДн:

– срок хранения для бумажных носителей ПДн, устанавливается согласно требованиям нормативно-правовой базы и федеральных законов, в зависимости от состава ПДн;

– бумажные носители ПДн хранятся в специализированных железных шкафах или сейфах;

– запрещается хранение бумажных носителей ПДн в местах, доступных для ознакомления посторонними лицами;

– Сотруднику Банка, выполняющему обработку ПДн с использованием бумажных носителей ПДн, запрещается хранить их на своем рабочем месте.

В Банке установлены следующие требования к уничтожению бумажных носителей ПДн:

– уничтожение бумажных носителей ПДн должно проводиться методами и способами, исключающими возможность полного или частичного восстановления данных носителей, например, при помощи технических средств (уничтожителей бумаги);

– ответственным лицом за уничтожение бумажных носителей ПДн назначается сотрудник Банка распорядительным документом Председателя Правления Банка;

– уничтожение бумажных носителей ПДн должно оформляться актом.

К неавтоматизированной обработке ПДн допускаются Сотрудники Банка, подписавшие «Соглашение о неразглашении персональных данных Клиента» и/или подписавшие «Соглашение о неразглашении персональных данных Сотрудника»;

6.2 Требования к организации неавтоматизированной обработки персональных данных

Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы. В случае обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Для типовых форм бумажных носителей ПДн (анкет, договоров), характер информации в которых предполагает или допускает включение в них ПДн, в Банке соблюдаются следующие условия:

– типовая форма бумажного носителя ПДн или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес Банка, фамилию, имя, отчество и адрес Субъекта и/или Сотрудника Банка, предоставляющих ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых Банком способов обработки ПДн;

– типовая форма бумажного носителя ПДн должна предусматривать поле, в котором Субъект и/или Сотрудник Банка, предоставляющий ПДн, может поставить отметку о своем согласии на неавтоматизированную обработку ПДн.

Уточнение персональных данных при осуществлении их неавтоматизированной обработки в Банке производится путем обновления или изменения данных на бумажном

носителе ПДн, либо путем изготовления нового бумажного носителя ПДн с уточненными ПДн.

Неавтоматизированная обработка ПДн в Банке должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения персональных данных (бумажных носителей ПДн).

При хранении бумажных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

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

7.1. 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.

7.2. 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 обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.3. 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, обязан прекратить неправомерную обработку персональных данных или обеспечить 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, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Банк обязан 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.

7.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Банк обязан с момента выявления такого инцидента

Банком, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Банком на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

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

7.5. В случае достижения цели обработки персональных данных Банк обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и уничтожить персональные данные или обеспечить 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 Законом №152-ФЗ или другими федеральными законами.

7.6. 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, уничтожить персональные данные или обеспечить 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 Законом №152-ФЗ или другими федеральными законами.

7.7. В случае обращения субъекта персональных данных к Банку с требованием о прекращении обработки персональных данных Банк обязан в срок, не превышающий десяти рабочих дней с даты получения Банком соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Закона № 152-ФЗ. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

7.8. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5.1 статьи 21 Закона № 152-ФЗ, 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.

7.9. Подтверждение уничтожения персональных данных в случаях, предусмотренных пунктом 7 Публичной политики, осуществляется в соответствии с требованиями, установленными приказом Роскомнадзора от 28.10.2022 N 179 "Об утверждении Требований к подтверждению уничтожения персональных данных".

8. Принципы обработки персональных данных с использованием сервисов веб-аналитики.

8.1 Банк обрабатывает персональные данные с использованием сервисов веб-аналитики «Bitrix 1с», (далее – сервисы веб-аналитики). Обработка персональных данных осуществляется следующими способами: сбор, систематизация, накопление, хранение, обновление, изменение, использование, передача третьим лицам (предоставление, доступ).

8.2. Субъектом обработки персональных данных с использованием сервисов веб аналитики являются пользователи официального сайта Банка, расположенного по адресу www.bankermak.ru (далее – пользователи).

8.3. Получение персональных данных для дальнейшей обработки с помощью сервисов веб-аналитики происходит при посещении официального сайта Банка. Данные пользователей официального сайта Банка собираются в автоматическом режиме с использованием файлов cookie, которые сохраняются в браузере компьютера или мобильного телефона после использования официального сайта Банка.

8.4. Банк обрабатывает персональные данные с использованием сервисов веб-аналитики в целях мониторинга и анализа пользовательской активности и использования официального сайта Банка, составления отчетов на основе полученной информации для дальнейшего качества пользовательского опыта.

8.5. Собранная информация о персональных данных не идентифицирует пользователя официального сайта Банка, за исключением случаев, когда одновременно с указанной ниже информацией пользователь указывает свое имя. Перечень обрабатываемых персональных данных пользователя с использованием сервисов веб-аналитики:

- IP-адрес пользователя
- файлы cookie;
- географическое положение (местонахождение);

9. Заключительные положения

9.1. Публичная политика вступает в силу с момента ее утверждения Правлением Банка. С момента вступления в силу настоящей Публичной политики, утрачивает силу Публичная политика по обработке и защите персональных данных Акционерного общества Нижневартовский городской банк «Ермак» от 16 января 2023 года.

9.2. В случае изменения действующего законодательства, изменения нормативных актов Центрального банка Российской Федерации настоящая Публичная политика действует в части, не противоречащей вновь принятым нормативным актам и действующему законодательству.

9.3. Изменения и дополнения в Публичную политику вносятся на основании решения Правления Банка. Ответственным за внесение изменений является Начальник службы Информационной Безопасности.

Составил:
Начальник службы
Информационной Безопасности  Ниценко Д. Н.