Приложение №3 к
«Политике информационной безопасности»
АО «Райффайзенбанк»

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ АО «РАЙФФАЙЗЕНБАНК»

ВЕРСИЯ 3.3

(Утверждено Председателем Правления АО «Райффайзенбанк» Мониным С.А. 15.03.2019 г.)

1. Введение и цели

Целью настоящей Политики в отношении обработки персональных данных АО «Райффайзенбанк» (далее – «Политика») является формулировка основных принципов и подходов к обработке и защите персональных данных, обрабатываемых АО «Райффайзенбанк» (далее - «Банк») в соответствии с требованиями законодательства Российской Федерации.

Политика распространяется на всех сотрудников Банка, включая временных сотрудников, задействованных в процессе обработки, в том числе при хранении персональных данных, и является обязательной для исполнения.

Положения настоящей Политики применяются в отношении персональных данных субъектов персональных данных.

2. Список терминов, определений, сокращений

Термин/ Сокращение	Определение
блокирование персональных данных	временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
информационная система персональных данных	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
обезличивание персональных данных	действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
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)
предоставление персональных данных	действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц
субъект персональных	соискатели; работники, состоящие в трудовых отношениях с банком; близкие родственники работников; уволенные

данных	сотрудники; лица, оказывающие банку услуги в соответствии с гражданско-правовыми договорами; потенциальные клиенты, заявки на кредиты которых рассматривает банк; физические лица, являющиеся клиентами банка, которым оказываются предусмотренные законодательством РФ банковские услуги (заемщики, вкладчики и другие), а также состоящие в иных договорных отношениях с банком; сотрудники клиентов-юридических лиц и индивидуальных предпринимателей, а также иные физические лица, персональные данные которых стали известны банку в ходе осуществления им банковской и хозяйственной деятельности
трансграничная передача персональных данных	передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
уничтожение персональных данных	действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

3. Положения Политики

Цели обработки персональных данных должны быть четко заявлены субъектам персональных данных и должны неукоснительно соблюдаться в течение всего жизненного цикла персональных данных. Объем и характер обрабатываемых персональных данных должны соответствовать целям их обработки. Недопустимо обрабатывать избыточные персональные данные, по отношению к заявленным целям обработки.

Обработка персональных данных должна осуществляться только с согласия субъекта персональных данных и в порядке, установленном действующим законодательством. Исключение составляют случаи, предусмотренные действующим законодательством Российской Федерации, в частности следующие:

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

- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

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

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

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

- обработка персональных данных необходима для осуществления прав и законных интересов 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;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях. За исключением обработки 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, которая допускается только при условии предварительного согласия субъекта персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

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

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", Банк обязан обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

В случае, если Банк на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных» №152-ФЗ от 27 июля 2006 г.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, когда субъект персональных данных дает непосредственное письменное согласие на обработку специальных категорий персональных данных.

Обработка специальных категорий персональных данных должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

Банк обязан предоставить сведения о наличии персональных данных по соответствующему запросу от субъекта персональных данных, при этом в этих сведениях не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

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

- подтверждение факта обработки персональных данных Банком, а также правовые основания и цель такой обработки;
- способы обработки персональных данных, применяемые Банком;
- 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;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения
- иные сведения, предусмотренные требованиями действующего законодательства Российской Федерации.

Обработка персональных данных в целях продвижения продуктов и услуг Банка путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных, при этом Банк должен иметь возможность доказать получение этого согласия. В случае соответствующего требования субъекта персональных данных, Банк обязан немедленно прекратить их обработку в указанных выше целях.

Любое распространение персональных данных должно производиться исключительно с согласия субъекта персональных данных, если иное не установлено законодательством (в частности, данные, предоставляемые следственным органам по результатам решений соответствующих инстанций).

В случае выявления обработки неточных персональных данных при обращении или запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных Банк обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, или обеспечить 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.

В случае подтверждения факта неточности персональных данных Банк на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить

персональные данные и снять их блокирование. В случае выявления неправомерной обработки персональных данных при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных Банк обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения такого запроса на период проверки.

В случае выявления неправомерной обработки персональных данных Банк в срок, регламентированный законодательством, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Банк в срок, регламентированный законодательством, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Банк обязан уведомить субъекта персональных данных или его законного представителя, а в случае поступления соответствующего запроса от уполномоченного органа по защите прав субъектов персональных данных, также уведомить указанный орган.

Персональные данные субъектов персональных данных должны подвергаться гарантированному уничтожению в случаях, когда обработка, в том числе и хранение этих данных более не требуется ни для бизнеса Банка, ни для соблюдения требований законодательства, а также в случае получения Банком отзыва согласия на обработку своих персональных данных, если это не противоречит требованиям законодательства и взаимоотношений субъекта персональных данных с Банком.

В ходе своей деятельности Банк может осуществлять трансграничную передачу персональных данных в Австрийскую Республику и Республику Румыния. Банк должен удостовериться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях, предусмотренных действующим законодательством Российской Федерации.

Следует иметь в виду, что в соответствии с законодательством Российской Федерации, возможность осуществления передачи персональных данных за пределы Российской Федерации может быть запрещена или ограничена уполномоченными органами государственной власти в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

4. Меры направленные на обеспечение выполнения требований по защите персональных данных

Деятельность Банка по обеспечению защиты персональных данных должна соответствовать требованиям действующего законодательства Российской Федерации и обеспечивать конфиденциальность и безопасность персональных данных при их обработке.

Перечень законодательных и подзаконных актов, а также требований регулирующих органов, имеющих отношение к деятельности Банка в области защиты персональных данных, должен быть документирован и регулярно обновляться.

Ответственность за ведение и обновление указанного перечня возлагается на Отдел информационной безопасности Управления экономической безопасности.

В Банке принимаются следующие меры по обеспечению выполнения требований по защите персональных данных:

- издаются внутренние нормативные документы Банка по вопросам обеспечения защиты персональных данных и их обработки, а также создаются локальные документы устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- осуществляется ознакомление работников Банка с внутренними нормативными документами, локальными документами, действующим законодательством регламентирующими, в частности, вопросы защиты персональных данных и их обработки.

С целью обеспечения безопасности персональных данных при их обработке, Банк принимает организационные и технические меры для защиты персональных данных от неправомерного и случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, в частности:- создана модель угроз персональных данных;

- применяются технические средства защиты информации;

- осуществляется оценка эффективности принимаемых мер по обеспечению безопасности ;

- проводятся мероприятия по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер по предотвращению такого доступа;

- обеспечивается возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; уничтожения, изменения, блокирования, копирования, а также от иных неправомерных действий в отношении персональных данных;

- осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

- устанавливаются правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечивается регистрация и учет действий, совершаемых с персональными данными в информационных системах персональных данных;

- иные меры.

Все отступления от Политики расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством, внутренними нормативными документами Банка или соглашением сторон.