

УТВЕРЖДЕНО:

Решением Совета директоров
АО «Сити Инвест Банк»
Протокол № 12/2017 от 04 июля 2017 г.
Председатель Совета директоров

_____ Гольдфарб М.В.

Политика
в отношении обработки персональных данных
АО «Сити Инвест Банк»

г. Санкт-Петербург

2017 г.

1. Общие положения

1.1. Политика в отношении обработки персональных данных АО «Сити Инвест Банк» (далее – Банк) представляет собой документ, разработанный с целью обеспечения и защиты прав и свобод человека при обработке персональных данных и обеспечения безопасности и конфиденциальности такой информации (далее – Политика).

1.2. Данная Политика основывается на требованиях законодательства Российской Федерации.

1.3. Политика распространяется на всех сотрудников Банка и является обязательной для исполнения.

1.4. К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу - субъекту персональных данных, обрабатываемая Банком для достижения заранее определенных целей.

1.5. Банк, а также его должностные лица и Работники несут гражданско-правовую, административную и иную ответственность за несоблюдение принципов и условий обработки персональных данных физических лиц, а также за разглашение или незаконное использование персональных данных в соответствии с законодательством Российской Федерации.

1.6. Политика является общедоступной и подлежит размещению на официальном сайте Банка или иным образом обеспечивается неограниченный доступ к настоящему документу.

2. Правовые основания обработки персональных данных.

Настоящая Политика по обработке персональных данных АО «Сити Инвест Банк» разработана, в том числе, в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности», Федеральным законом от 26.07.2006 № 135-ФЗ «О защите конкуренции», Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Постановлением Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных," инструкцией Банка России и иными нормативно-правовыми актами, регулирующими отношения связанные с персональными данными.

3. Список терминов

Банк – АО «Сити Инвест Банк», юридическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных;

персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями, а также в связи с осуществлением Банком деятельности, предусмотренной уставом и действующим законодательством;

субъект персональных данных – лицо, персональные данные которого обрабатываются Банком;

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;

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

обработка персональных данных без использования средств автоматизации- обработка персональных данных, осуществляемая без средств вычислительной техники

конфиденциальность персональных данных - обязательное, требование не допускать распространения персональных данных без согласия субъекта персональных данных или иного законного основания;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

использование персональных данных - действия (операции) с персональными данными, совершаемые сотрудниками Банка в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных, либо иным образом затрагивающих их права и свободы или права и свободы других 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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных (бумажные или электронные);

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

общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности (например, данные телефонных и иных справочников, информация в которых публикуется с разрешения владельца персональных данных);

информация - сведения (сообщения, данные) независимо от формы их предоставления;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

4. Общие принципы обработки персональных данных.

- законности заранее определенных конкретных целей и способов обработки персональных данных;
- обеспечения надлежащей защиты персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- соответствия объема, характера и способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- хранения персональных данных в форме, позволяющей определить Субъекта персональных данных, не дольше, чем этого требуют цели их обработки;
- уничтожения или обезличивания персональных данных по достижении целей их обработки, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных;
- обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

5. Цели обработки персональных данных

Банк осуществляет обработку персональных данных в целях:

- осуществления банковских операций и сделок в соответствии с Уставом Банка и выданными Банку лицензиями на совершение банковских и иных операций;
- заключения с Субъектом персональных данных любых договоров и их дальнейшего исполнения;
- проведения Банком акций, опросов, исследований;
- предоставления Субъекту персональных данных информации об оказываемых Банком услугах, о разработке Банком новых продуктов и услуг; информирования Клиента о предложениях по продуктам и услугам Банка;
- ведения кадровой работы и организации учета работников Банка;
- привлечения и отбора кандидатов на работу в Банке;

- формирования статистической отчетности, в том числе для предоставления Центральному Банку России;
- для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей.

6. Перечень субъектов персональных данных, объем и категории персональных данных, обработка которых осуществляется Банком.

6.1. Банк осуществляет обработку персональных данных следующих категорий Субъектов персональных данных:

- физические лица, являющиеся Кандидатами;
- физические лица, являющиеся работниками Банка, а также прекратившие трудовые отношения с Банком;
- физические лица, осуществляющие выполнение работ по оказанию услуг и заключившие с Банком договор гражданско-правового характера;
- физические лица, входящие в органы управления Банка;
- представители клиентов или потенциальных клиентов Банка;
- физические лица, являющиеся клиентами Банка или потенциальными клиентами Банка
- физические лица, персональные данные которых сделаны ими общедоступными, а их обработка не нарушает их прав и соответствует требованиям, установленным Законодательством о персональных данных;
- иные физические лица, выразившие согласие на обработку Банком их персональных данных или физические лица, обработка персональных данных которых необходима Банку для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей.

6.2. Объем и категория обрабатываемых персональных данных зависит от заявленной цели обработки. Перечень обрабатываемых персональных данных в зависимости от целей обработки установлен Банком в типовых формах согласия на обработку персональных данных, утверждаемых Председателем Правления.

6.3. Банк не осуществляет обработку специальных категорий персональных данных, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, интимной жизни, судимости физических лиц, если иное не установлено законодательством Российской Федерации.

6.4. Обработка специальной категории персональных данных, касающихся состояния здоровья Субъекта персональных данных, осуществляется с согласия Субъекта персональных данных в письменной форме, а также без такового, в случаях установленных действующим законодательством.

7. Права и обязанности участников отношений по обработке персональных данных:

7.1. Права субъектов персональных данных:

- получать информацию, касающуюся обработки его персональных данных, в порядке, форме и сроки, установленные Законодательством о персональных данных;
- требовать уточнения своих персональных данных, их Блокирования или Уничтожения в случаях, установленных Законодательством о персональных данных
- принимать предусмотренные законом меры по защите своих прав;
- отозвать свое согласие на обработку персональных данных.
- иные права, предусмотренные Законодательством о персональных данных.

7.2. Банк имеет право:

- обрабатывать персональные данные Субъекта персональных данных в соответствии с заявленной целью;
- требовать от Субъекта персональных данных предоставления достоверных персональных данных;
- ограничить доступ Субъекта персональных данных к его персональным данным в случае, если Обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, доступ Субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц, а также в иных случаях, предусмотренных законодательством Российской Федерации;
- обрабатывать общедоступные персональные данные физических лиц;

- осуществлять обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации;

7.3. Банк обязан:

- принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами.

8. Порядок и условия обработки персональных данных.

8.1. При обработке персональных данных Банк осуществляет следующие действия:

сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных и иные действия не запрещенные законодательством о персональных данных.

8.2. Банк обрабатывает персональные данные как с использованием средств автоматизации, так и без их использования.

8.3. Банк осуществляет трансграничную передачу персональных данных с целью выполнения договорных обязательств и в соответствии с законодательством Российской Федерации.

8.4. Банк осуществляет передачу персональных данных государственным органам в рамках их полномочий в соответствии с законодательством Российской Федерации.

8.5. Обработка персональных данных прекращается при достижении целей такой обработки, а также по истечении срока, предусмотренного действующим законодательством, договором, или согласием Субъекта персональных данных на обработку его персональных данных. При отзыве Субъектом персональных данных согласия на обработку его персональных данных обработка осуществляется только в пределах, необходимых для исполнения заключенных с ним договоров и в целях, предусмотренных законодательством Российской Федерации.

Срок действия согласия на обработку персональных данных для клиентов и потенциальных клиентов Банка, а также их представителей, лиц, заключивших с Банком договора гражданско-правового характера составляет пять лет с даты его выдачи, а в случае наличия заключенных договоров между субъектом персональных данных и Банком - в течение пяти лет с даты окончания соответствующих договоров.

8.6. Обработка персональных данных осуществляется с соблюдением конфиденциальности, под которой понимается обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

8.7. Согласие может быть отозвано путем направление в адрес Банка письменного отзыва согласия по почте заказным письмом с уведомлением о вручении, так и любым иным путем не запрещенным законом. Согласие на обработку может быть отозвано относительно как всех персональных данных субъекта, так и на часть обрабатываемых персональных данных.

8.8. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Банк обязан прекратить их обработку или обеспечить 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 в срок, не превышающий 30 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.

В случае отсутствия возможности уничтожения персональных данных, в течение вышеуказанного срока, 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 действующим законодательством.

8.9. В случае обращения Субъекта персональных данных или его представителя по поводу неточностей персональных данных Банк обязан в срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, внести в них необходимые изменения.

8.10. В случае обращения Субъекта персональных данных или его представителя по поводу неправомерности обработки персональных данных Банк обязан в срок, не превышающий 7 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, уничтожить такие персональные данные.

8.11. Условия хранения персональных данных, содержащихся на бумажных носителях, установлены внутренними положениями Банка, в том числе положением о работе архива.

8.12. Условия хранения персональных данных, содержащихся в электронном виде, регламентируются внутренними инструкциями Управления автоматизации.

8.13. При осуществлении хранения персональных данных Банк обязан использовать базы данных, находящиеся на территории Российской Федерации.

8.14. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению в порядке, установленном действующим законодательством.

9. Меры принимаемые Банком для защиты персональных данных.

9.1. 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.

9.2. К таким мерам по обеспечению безопасности персональных данных, принимаемым Банком, в частности, относятся:

- назначение в Банке ответственного за организацию обработки персональных данных;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- учет машинных носителей персональных данных;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по недопущению подобных инцидентов в дальнейшем;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

10. Заключительные положения

10.1. Настоящая Политика является обязательной для выполнения всеми сотрудниками Банка в части выполнения ими своих должностных обязанностей, знания нормативных и законодательных актов и соблюдения внутрибанковского документооборота.

10.2. В случае изменения действующего законодательства Российской Федерации, нормативных документов Банка России и внутрибанковских документов настоящая Политика действует в части, не противоречащей вновь принятым нормативным документам.

10.3. Изменения в настоящую Политику вносятся на основании решения Совета директоров Банка.

10.4. Настоящая Политика вступает в силу с даты ее утверждения.