

УТВЕРЖДАЮ
Председатель Правления
«СДМ – Банк» (ПАО)
Солнцев М.М.

«07» июля 2015 г

**ПОЛИТИКА «СДМ-Банк» (ПАО) В ОТНОШЕНИИ ОБРАБОТКИ
ПЕРСОНАЛЬНЫХ ДАННЫХ**

Редакция 2.0.

Утверждено Приказом от «07» июля 2015 г. № 50-187/2015

Разработчик: Начальник отдела сопровождения
гражданско-правовых и налоговых вопросов Бобрицкий Ф.Г.

ОГЛАВЛЕНИЕ:

1. Общие положения	3
2. Основные понятия.....	3
3. Порядок обработки персональных данных.....	4
4. Применяемые процедуры при обработке персональных данных.....	5
5. Сведения о реализуемых требованиях к защите персональных данных.....	7

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящая Политика обработки персональной информации (далее по тексту – «Политика») действует в отношении обработки и обеспечения защиты персональных данных.

1.2. Настоящая Политика определяет порядок и описание применяемых банком процедур обработки персональных данных работников банка и иных лиц, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных.

1.3. Персональные данные не могут быть использованы банком в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

1.4. Настоящая Политика является публичным документом и подлежит размещению на сайте банка в общем доступе.

2. ОСНОВНЫЕ ПОНЯТИЯ.

Оператор персональных данных (далее оператор) - в рамках настоящей Политики оператором является – «СДМ-Банк» (ПАО);

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

Субъект - субъект 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;

Конфиденциальность персональных данных - обязательное для соблюдения назначенным ответственным лицом, получившим доступ к персональным данным субъектов, требование не допускать их распространения без согласия субъекта или иного законного основания;

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц»

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

Блокирование персональных данных - 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 и (или) в результате которых уничтожаются материальные носители персональных данных;

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

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

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

3. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

3.1. В банке установлен единый порядок обработки персональных данных для всех ресурсов.

3.2. Банком принимаются к обработке персональные данные, полученные в установленном законом порядке.

3.3. В банке установлен конкретный перечень персональных данных, которые могут обрабатываться и получение иных персональных данных запрещено.

3.4. Обработка персональных данных в информационной системе персональных данных работниками банка осуществляется в целях, принятия решений или совершении иных действий, порождающих юридические последствия в отношении субъекта персональных данных и иных лиц; содействия сотрудникам в обучении, продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества; предупреждения, выявления и пресечения деяний, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

3.5. Банк осуществляет обработку персональных данных с использованием средств автоматизации и без использования средств автоматизации.

3.6. 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).

3.7. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

3.8. 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.

3.9. Персональные данные субъекта хранятся в подразделении банка, которое отвечает за взаимодействие с субъектом. Персональные данные хранятся в бумажном виде в папках и находятся в сейфе или в металлическом шкафу, обеспечивающим защиту от несанкционированного доступа.

3.10. Персональные данные субъекта в подразделении банка могут также храниться в электронном виде в локальной компьютерной сети.

3.11. Банк вправе поручить обработку персональных данных третьему лицу при условии наличия на это согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, на основании заключаемого с этим лицом договора, условием которого является соблюдение конфиденциальности и неразглашения персональных данных.

3.12. Представители органов государственной власти (в том числе, контролирующих, надзорных, правоохранительных и иных органов), получают доступ к персональным данным, обрабатываемым в банке, в объеме и порядке, установленном законодательством Российской Федерации.

3.13. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, а также в иных случаях установленных законодательством.

3.14. Уточнение персональных данных при осуществлении их обработки производится путем обновления или изменения данных.

3.15. Трансграничная передача персональных данных банком не осуществляется.

4. ПРИМЕНЯЕМЫЕ ПРОЦЕДУРЫ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

- 4.1. Процедура предоставления доступа субъекта к персональным данным.
 - 4.1.1. Субъект или его законный представитель имеют право на получение от банка информации, установленной законодательством, касающейся обработки персональных данных субъекта.
 - 4.1.2. Запросы (обращения) субъектов и их законных представителей фиксируются в журнале учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных.
 - 4.1.3. 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 оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.
 - 4.1.4. Банк предоставляет ответ на запрос субъекта или его представителя, а также предоставляет возможность ознакомления с персональными данными субъекта в течение тридцати дней с даты получения запроса.
- 4.2. Процедура внесения изменений в персональные данные:
 - 4.2.1. С целью обеспечения точности, достоверности и актуальности персональных данных, в том числе по отношению к целям их обработки субъект персональных данных вправе требовать от банка уточнения его персональных данных.
 - 4.2.2. Процедура направления обращения субъекта и ответа банка на данное обращение осуществляется в порядке указанном п.4.1.2. - 4.1.4. настоящей Политики.
 - 4.2.3. В случае подтверждения факта неточности персональных данных банк на основании сведений, представленных субъектом или его представителем либо уполномоченным органом по защите прав субъектов, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений.
- 4.3. Процедура уничтожения, обезличивания либо блокировки персональных данных:
 - 4.3.1. Субъект вправе требовать от банка блокирования, обезличивания или уничтожения своих персональных данных в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.
 - 4.3.2. Процедура направления обращения субъекта и ответа банка на данное обращение осуществляется в порядке указанном п.4.1.2. - 4.1.4. настоящей Политики.
 - 4.3.3. В случае выявления банком неправомерной обработки персональных данных при обращении субъекта или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту, или обеспечить их блокирование с момента такого обращения или получения указанного запроса на период проверки.
 - 4.3.4. В случае выявления неправомерной обработки персональных данных, осуществляемой банком, банк в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

- 4.3.5. По достижении цели обработки персональных данных банк прекращает обработку персональных данных и уничтожает персональные данные.
- 4.4. Процедура обработки обращений субъектов и уполномоченного органа.
 - 4.4.1. Все поступающие в банк с нарочными, курьерами, по почте запросы субъектов, их представителей и государственного органа подлежат обязательной регистрации в «Журнале учета запросов (обращений)» в день поступления запроса в банк.
 - 4.4.2. После регистрации вновь поступившего запроса он передается ответственному сотруднику для подготовки ответа.
 - 4.4.3. Ответственный сотрудник изучает поступивший запрос на предмет его соответствия действующему законодательству и готовит соответствующий ответ (о наличии персональных данных субъекта и возможности ознакомления с ними; о внесении уточнений в персональные данные субъекта; блокировке персональных данных субъекта; уничтожении персональных данных субъекта).
 - 4.4.4. Банк предоставляет ответ на запрос субъекта, его представителя и уполномоченного органа в течение тридцати дней с даты получения запроса.
- 4.5. Процедура получения согласия субъекта на обработку его персональных данных и на передачу обработки его персональных данных третьим лицам.
 - 4.5.1. Субъект принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе.
 - 4.5.2. Отдельные документы, на основании которых банк получает от субъекта персональные данные, должны содержать письменное согласие субъекта.
 - 4.5.3. Если иное не предусмотрено законом, передача третьим лицам персональных данных субъекта для их обработки, возможна только с письменного согласия субъекта.

Согласие может быть получено банком в момент предоставления субъектом своих персональных данных, а также после их предоставления при получении от субъекта письменного положительного ответа на соответствующий запрос банка.
- 4.6. Процедуры работы в банке с материальными носителями персональных данных и их передачи между пользователями:
 - 4.6.1. Персональные данные на бумажных носителях хранятся в папках и находятся в сейфе или в металлическом шкафу, обеспечивающим защиту от несанкционированного доступа.
 - 4.6.2. Доступ к персональным данным субъектов, имеют сотрудники определенные внутренним документом банка.
 - 4.6.3. Все машинные носители данных, на которые записываются персональные данные, обязательно регистрируются и учитываются.
 - 4.6.4. Хранение машинных носителей осуществляется в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.
 - 4.6.5. Материальные носители персональных данных выдаются только сотрудникам, допущенным к обработке персональных данных. По завершению работы материальные носители персональных данных сдаются ответственному для их хранения.
- 4.7. Процедура уведомления уполномоченного органа по защите прав субъектов об обработке персональных данных:
 - 4.7.1. В соответствии с Федеральным законом № 152-ФЗ от 27.07.2006 г. «О персональных данных» банк уведомил уполномоченный орган по защите прав субъектов об обработке персональных данных.
 - 4.7.2. Уполномоченным органом по защите прав субъектов банку в реестре операторов, осуществляющих обработку персональных данных, присвоен регистрационный номер 10-0096564.
- 4.8. Процедура применения в банке типовых форм с целью сбора персональных данных.

4.8.1. С целью недопущения получения персональных данных субъекта в объеме превышающем установленный, сбор персональных данных субъектов в банке осуществляется строго на основании утвержденных типовых форм.

5. СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

5.1. В Банке уделяется большое внимание к обеспечению необходимого и достаточного уровня безопасности обрабатываемых ресурсов персональных данных, соблюдения их конфиденциальности, сохранности материальных носителей персональные данные.

5.2. В Банке созданы все необходимые условия для защиты информации, отнесенной к персональным данным.

5.3. Банк предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных, а именно:

5.3.1. Назначены ответственный сотрудник за организацию обработки и обеспечение безопасности персональных данных;

5.3.2. Введен режим защиты помещений, в которых осуществляется обработка и хранение материальных носителей персональных данных;

5.3.3. Определен круг лиц, имеющих право обработки персональных данных, а также доступа в помещения в которых обрабатываются персональные данные, разработаны инструкции пользователям по защите персональных данных, антивирусной защите;

5.3.4. Определены требования к сотрудникам банка, уполномоченным обрабатывать персональные данные, документально закреплена степень их ответственности за обеспечение безопасности персональных данных;

5.3.5. Проведено ознакомление сотрудников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации по обеспечению безопасности персональных данных и требованиями к защите персональных данных, внутренним положением банка в отношении обработки персональных данных. Проводится периодическое обучение указанных работников правилам обработки персональных данных;

5.3.6. Осуществление в банке внутреннего контроля соответствия обработки персональных данных Федеральному закону № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных;

5.3.7. Предприняты необходимые и достаточные технические меры для обеспечения безопасности персональных данных от их случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий:

- Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

- Применение банком прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- введена система разграничения доступа;

- установлена защита от несанкционированного доступа к автоматизированным рабочим местам, информационным сетям и базам персональных данных;

- установлена защита от воздействия вредоносных программ;

- на регулярной основе осуществляется резервное копирование информации в целях восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- организована система проверки соответствия системы защиты персональных данных, проводится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.