УТВЕРЖДЕНО
Решением Правления

Протокол № 827 от 09.08.2021 г.

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ АО "ТОЙОТА БАНК"

Автор	В. Волчков
Согласовано	Президент _____ Александр Колошенко (подпись)
Вступает в силу	с даты утверждения Правлением
Редакция №	1
Хранение	Бумажный документ с подписями – Комплаенс-контролер Электронный документ – G:\Book of Procedures\Политики и процедуры\1800 Информационная безопасность\
Область действия (на кого распространяется)	Все сотрудники АО "Тойота Банк"

АННОТАЦИЯ

Настоящая Политика обеспечивает исполнение АО «Тойота Банк» и его сотрудниками требований действующего законодательства РФ в области обработки персональных данных, а также определяет цели, условия и порядок обработки персональных данных, устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в Банке как с использованием средств автоматизации так и без использования таких средств.

Настоящая Политика разработана в соответствии с требованиями действующего законодательства РФ в области обработки и обеспечения безопасности персональных данных.

Политика является общедоступной и подлежит размещению на официальном сайте Банка в сети Интернет.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 5
ЗАДАЧА 6
ОТВЕТСТВЕННЫЕ 6
1. Цель Политики 6
2. Общие положения, принципы и цели обработки персональных данных 6
3. Функции Банка при осуществлении обработки персональных данных 8
4. Способы обработки и перечень действий с персональными данными 8
5. Субъекты и категории персональных данных 9
6. Обеспечение безопасности персональных данных 10
7. Права субъектов персональных данных 11
8. Обязанности сотрудников, допущенных к обработке ПДн 12
9. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Банка в области персональных данных, в том числе требований к защите персональных данных 12

ВВЕДЕНИЕ

Политика обработки персональных данных в АО «Тойота Банк» (далее по тексту – Политика, Банк - соответственно) разработана в целях обеспечения безопасности персональных данных, направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

Политика разработана с учетом рекомендаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2017 «Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом «О персональных данных».

Политика принята в соответствии со следующими основными нормативно-правовыми актами:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности».
- Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах».
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России № 55, ФСБ России № 86, Мининформсвязи России № 20 от 13 февраля 2008 г. «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти;
- Устав;
- Политика информационной безопасности Банка и иные внутренние документы Банка.

Настоящая Политика является основой для организации работы по обработке персональных данных в Банке и для разработки локальных нормативных актов, регламентирующих в Банке вопросы обработки персональных данных.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящей Политике используются следующие термины и определения:

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 настоящим Федеральным законом.

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено с помощью персональных данных.

Оператор – АО «Тойота Банк», самостоятельно организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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), удаление, уничтожение, обезличивание, блокирование персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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.

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

Уничтожение (удаление) персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе (удаление) персональных данных и (или) в результате которых уничтожаются материальные носители (уничтожение) персональных данных.

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

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

Неавтоматизированная обработка персональных данных – обработка персональных данных без использования средств вычислительной техники.

Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных.

Специальные категории персональных данных – данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

ЗАДАЧА

Задача настоящей Политики заключается в определении основных принципов, целей, условий и способов обработки персональных данных, перечней субъектов и обрабатываемых в Банке персональных данных, функций Банка и обязанностей сотрудников Банка при обработке персональных данных, прав субъектов персональных данных, а также реализуемых в Банке требований к защите персональных данных.

ОТВЕТСТВЕННЫЕ

За выполнение положений настоящего документа отвечает руководство Банка и все сотрудники Банка, в пределах своих полномочий, вне зависимости от занимаемой должности.

1. Цель Политики

1.1. Целью настоящей Политики является обеспечение соответствия процесса обработки и защиты персональных данных в Банке требованиям действующего законодательства Российской Федерации.
1.2. Действие Политики распространяется на всех сотрудников Банка и руководство, на все бизнес-процессы Банка, связанные с обработкой и защитой персональных данных.
1.3. Каждый сотрудник подтверждает в электронном виде или личной подписью, что он ознакомлен с положениями настоящей Политики.

2. Общие положения, принципы и цели обработки персональных данных

2.1. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
2.2. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать соответствующие меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
2.3. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.4. В случае достижения цели обработки ПДн, если иное не предусмотрено законодательством Российской Федерации, Банк прекращает обработку и производит их уничтожение, или обеспечивает прекращение обработки и уничтожение ПДн, которые обрабатывались третьими лицами на основании договора с Банком, в порядке, установленном законодательством Российской Федерации.

2.5. Банк осуществляет трансграничную передачу ПДн в случаях, предусмотренных законодательством Российской Федерации, а также на основе соответствующих соглашений с международными и иностранными организациями, закрепляющих соответствующую защиту прав субъектов ПДн, в том числе в части обеспечения конфиденциальности ПДн как составной части конфиденциальной информации, обмен которой производится.

2.6. Банк осуществляет обработку Персональных данных на основе следующих принципов:

- законности целей и способов Обработки Персональных данных;
- добросовестности, законности, справедливости, и конфиденциальности при Обработке Персональных данных;
- соответствия целей Обработки Персональных данных целям, заранее определенным и заявленным при сборе Персональных данных, а также полномочиям Банка;
- соответствия объема и характера обрабатываемых Персональных данных, 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 созданных для несовместимых между собой целей баз данных Информационных систем Персональных данных.

2.7. Персональные данные обрабатываются:

- в целях исполнения требований действующего законодательства Российской Федерации;
- в целях осуществления банковских операций и иной деятельности в соответствии с Уставом и выданными Банку лицензиями;
- в целях регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации (обрабатываются также и иные сведения, если такие сведения предусмотрены федеральными законами в указанной системе, и биометрические персональные данные гражданина Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации):
- в целях организации ведения кадрового учета;
- в целях организации ведения бухгалтерского и налогового учета;
- в целях изготовления визитных карточек;
- в целях обеспечения безопасности при осуществлении пропускного режима и пребывании на территории Банка;
- в целях организации бронирования билетов и гостиниц сотруднику Банка, выезжающему в командировку;
- в целях исполнения заключенных гражданско-правовых договоров;
- в целях проведения предварительного собеседования с целью трудоустройства;
- в целях оформления договора добровольного медицинского страхования и страхования жизни от несчастного случая;

- в целях составления управленческой отчетности, формирования статистических отчетов, анализа данных, в целях функционирования официального сайта Банка, проведения ремаркетинга и осуществления статистических исследований и обзоров;
- в целях продвижения товаров и услуг;
- в целях ведения единого справочника корпоративных телефонов и корпоративной электронной почты на корпоративном информационном портале Банка;
- в иных законных целях, предусмотренных законодательством Российской Федерации.

3. Функции Банка при осуществлении обработки персональных данных

3.1. Банк принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Банка в области персональных данных.
3.2. Банк принимает 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.
3.3. Банк назначает лицо, ответственное за организацию обработки персональных данных.
3.4. Банк утверждает внутренние документы, определяющие вопросы обработки и защиты персональных данных.
3.5. Банк публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике.
3.6. Банк сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации
3.7. Банк прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных
3.8. Банк уведомляет уполномоченный орган по защите прав субъектов персональных данных (далее по тексту – Уполномоченный орган) до начала обработки персональных данных (далее -Уведомление), согласно статье 22 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». В случае изменения сведений, указанных в Уведомлении и предоставленных Уполномоченному органу, а также в случае прекращения обработки персональных данных Банк обязан уведомить об этом Уполномоченный орган в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.
3.9. Банк совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

4. Способы обработки и перечень действий с персональными данными

4.1. Перечень действий с персональными данными, которые могут осуществляться Банком при обработке персональных данных субъектов:

- сбор;
- запись;
- систематизация;

- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передача (распространение, предоставление, доступ);
- блокирование;
- удаление;
- уничтожение;
- распространение.

4.2. Обработка персональных данных в Банке осуществляется следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

5. Субъекты и категории персональных данных

5.1. Категории Субъектов персональных данных

Банк выделяет следующие категории субъектов персональных данных:

- физические лица, состоявшие или состоящие в договорных и иных гражданско-правовых отношениях с Банком;
- физические лица, состоящие в трудовых отношениях с Банком (далее – Сотрудники).
- иные субъекты персональных данных (для обеспечения реализации целей обработки, указанных в разделе 2 Политики).

5.2. Категории персональных данных Субъектов персональных данных.

Перечень обрабатываемых персональных данных определяется в соответствии с законодательством Российской Федерации и внутренними документами Банка с учетом целей обработки персональных данных, указанных в разделе 2 настоящей Политики.

Банк обрабатывает следующие категории персональных данных:

- общедоступные и (или) обезличенные персональные данные;
- специальные категории персональных данных:
  - сведения о состоянии здоровья;
  - сведения о судимости;
- биометрические персональные данные:
  - изображение лица (фотография и видеоизображение);
  - голос;
- разрешенные для распространения персональные данные;
- иные персональные данные.

5.3. Банк устанавливает правила (порядок) работы с Персональными данными, в том числе допустимые случаи обработки специальных категорий и биометрических Персональных данных, определяет для каждой цели обработки и категории субъектов Персональных данных содержание обрабатываемых в Банке Персональных данных и регламентирует вышеуказанные вопросы отдельными внутренними документами Банка.

5.4. В информационных системах Банка не осуществляется обработка персональных данных, относящихся к специальным категориям персональных данных, касающихся расовой,

национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости.

5.5. Неавтоматизированная обработка специальных категорий персональных данных, касающихся состояния здоровья, судимости, может осуществляться, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных.

6. Обеспечение безопасности персональных данных

6.1. Основной целью обеспечения безопасности Персональных данных является минимизация рисков и возможного ущерба (потерь) от их реализации, возникших вследствие возможной реализации внутренних и внешних угроз информационной безопасности Персональных данных и уязвимостей объектов защиты.

6.2. Основным условием реализации целей и задач обеспечения безопасности Персональных данных является обеспечение необходимого и достаточного уровня защиты Персональных данных. Защита Персональных данных осуществляется в Банке на основе следующих принципов:

- Законность – защита Персональных данных основывается на положениях и требованиях применимых законов, подзаконных актов, стандартов по защите Персональных данных.
- Системность – системный подход к построению системы защиты Персональных данных предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени компонентов, факторов, условий.
- Непрерывность совершенствования – предполагает постоянное совершенствование мер и средств защиты Персональных данных.
- Комплексность – безопасность Персональных данных обеспечивается комплексом правовых, организационных и технических мер, реализованных Банком.
- Своевременность – принимаемые Банком меры по обеспечению безопасности персональных данных должны быть приняты вовремя.
- Непрерывность – защита Персональных данных обеспечивается на всех этапах их обработки и во всех режимах функционирования систем Обработки Персональных данных.
- Разумная достаточность и адекватность – состояние и стоимость реализации мер защиты должны быть соизмеримы с рисками, связанными с Обработкой и характером защищаемых Персональных данных.
- Персональная ответственность – ответственность за обеспечение безопасности
- Персональных данных в Банке возлагается на руководство и на каждого сотрудника в пределах его полномочий.
- Минимизация полномочий – доступ к Персональным данным предоставляется сотрудникам Банка только в объеме, необходимом для выполнения их должностных обязанностей.
- Профессионализм и специализация – реализация мер по обеспечению безопасности Персональных данных и эксплуатации системы защиты должна осуществляться квалифицированными сотрудниками Банка.
- Знание и мотивация лиц, допущенных к Обработке Персональных данных, – Банк должен реализовать кадровую политику (тщательный подбор персонала и мотивация сотрудников), позволяющую исключить или минимизировать возможность нарушения безопасности Персональных данных своими сотрудниками.

- Обязательность оценки и контроля – неотъемлемой частью работ по защите Персональных данных является оценка эффективности системы защиты Персональных данных.

6.3. Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Банка.

6.4. Банк не осуществляет передачу, разглашение или распространение персональных данных без согласия субъекта, если иное не предусмотрено законодательством РФ. В Банке утвержден перечень должностных лиц, имеющих доступ и/или осуществляющих обработку персональных данных с использованием и/или без использования средств автоматизации.

6.5. Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. В том случае, если для выполнения банковского информационного технологического процесса, реализацию которого поддерживает информационная система персональных данных, нет необходимости в обработке определенных персональных данных, эти персональные данные должны быть удалены.

6.6. Для персональных данных, обрабатываемых в информационных системах Банка, должны быть установлены и документально определены уровни защищенности персональных данных.

7. Права субъектов персональных данных.

7.1. Субъекты персональных данных имеют право на:

- получение полной информации о персональных данных, обрабатываемых в Банке, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
- уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыв согласия на обработку персональных данных;
- принятие предусмотренных законом мер по защите своих прав;
- обжалование действия или бездействия Банка, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке;
- получение сведений о Банке как об Операторе, о месте его нахождения;
- осуществление иных прав, предусмотренных законодательством Российской Федерации.

7.2. Банк в обязательном порядке рассматривает все обращения субъектов ПДн.

7.3. Порядок обработки обращений и запросов субъектов ПДн (или их законных представителей) по вопросам обработки их ПДн и действий в случае запросов уполномоченного органа по защите прав субъектов ПДн или иных надзорных органов, осуществляющих контроль и надзор в области ПДн, устанавливается внутренними документами Банка.

7.4. Предоставление ПДн не должно нарушать конституционные права и свободы других лиц и в предоставляемых данных не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

7.5. В случае отзыва субъектом ПДн согласия на обработку его ПДн, если иное не предусмотрено законодательством Российской Федерации, Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если ПДн обрабатываются третьими лицами по договору с Банком). В случае, если сохранение ПДн более не требуется

для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если ПДн обрабатываются третьими лицами по договору с Банком) в порядке, установленном законодательством Российской Федерации о защите персональных данных.

8. Обязанности сотрудников, допущенных к обработке ПДн

Сотрудники, допущенные к обработке ПДн, обязаны:

- знать и неукоснительно выполнять положения настоящей Политики;
- обрабатывать ПДн только в рамках выполнения своих должностных обязанностей;
- не разглашать ПДн, полученные в результате выполнения своих должностных обязанностей, а также ставшие им известными по роду своей деятельности;
- пресекать действия других лиц, которые могут привести к разглашению (уничтожению, искажению) ПДн;
- выявлять факты разглашения (уничтожения, искажения) ПДн и уведомлять уполномоченных лиц Банка в соответствии с действующими внутренними процедурами Банка.

9. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Банка в области персональных данных, в том числе требований к защите персональных данных

9.1. Контроль за соблюдением законодательства Российской Федерации и внутренних документов Банка в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных

9.2. Лица, виновные в нарушении требований действующего законодательства о персональных данных, а также положений настоящей Политики несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.