

**ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«СБЕРБАНК РОССИИ»**

УТВЕРЖДЕНА
Постановлением Правления
ОАО «Сбербанк России»
Протокол от 29.04.2014 № 506 § 27

"29" апреля 2014г.

№ 3324

**ПОЛИТИКА
обработки персональных данных
в ПАО Сбербанк
(с учетом изменений №1 от 17.11.2016,
№2 от 04.07.2017)**

г. Москва
2014

Реквизиты ВНД

Наименование, номер ВНД	Политика обработки персональных данных в ПАО Сбербанк № 3324																					
Подразделение-разработчик ВНД	Департамент развития отношений с клиентами и вторичных продаж																					
Исполнитель ВНД	Левочкина Жанэт, 36-532																					
Код направления деятельности/код процесса	Б.1.2, Б.7.7, О.1.1, О.1.4, О.1.6.																					
Действие ВНД распространяется на подразделения	<input checked="" type="checkbox"/>	Центральный аппарат																				
	<input checked="" type="checkbox"/>	Территориальные банки																				
	<input checked="" type="checkbox"/>	Отделения банка																				
	<input checked="" type="checkbox"/>	Внутренние структурные подразделения Подразделения центрального подчинения																				
ВНД верхнего уровня																						
История ВНД																						
Номер редакции	Распорядительный документ, утверждающий /изменяющий ВНД																					
1	Постановление Правления ОАО "Сбербанк России" от 29.04.2014 № 506 §27																					
1/1	Постановление Правления ПАО Сбербанк от 17.11.2016 № 554 §29а																					
ВНД, которые утрачивают силу с выходом данного ВНД																						
Рассылка ВНД																						
<input checked="" type="checkbox"/>	Территориальные банки																					
	Подразделения Центрального аппарата (для конфиденциальных документов)																					
<input checked="" type="checkbox"/>	Подразделения центрального подчинения																					
Информация о полномочиях ТБ по изменению устанавливаемого порядка																						
<input checked="" type="checkbox"/>	Изменению не подлежит																					
	Возможны изменения порядка, установленного следующими разделами:																					
	Разделы																					
	Приложения																					
	Возможность изменения																					

СОДЕРЖАНИЕ

1. Общие положения	4
2. Цели обработки персональных данных.....	4
3. Классификация персональных данных и Субъектов персональных данных.....	5
4. Общие принципы обработки персональных данных.....	6
5. Основные участники системы управления процессом обработки персональных данных	7
6. Организация системы управления процессом обработки персональных данных	8
7. Заключительные положения	9
ПРИЛОЖЕНИЕ 1.....	10
ПРИЛОЖЕНИЕ 2.....	12
ПРИЛОЖЕНИЕ 3.....	13

1. Общие положения

1.1. Политика обработки персональных данных в ПАО Сбербанк (далее - Политика) разработана в соответствии с /1/, /2/, /3/, /4/, а также в соответствии с иными федеральными законами и подзаконными актами Российской Федерации, определяющими случаи и особенности обработки персональных данных и обеспечения безопасности и конфиденциальности такой информации (далее - Законодательство о персональных данных).

1.2. Политика разработана в целях реализации требований законодательства в области обработки и обеспечения безопасности персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Банке.

1.3. Политика устанавливает:

- цели обработки персональных данных;
- классификацию персональных данных и Субъектов персональных данных;
- общие принципы обработки персональных данных;
- основных участников системы управления процессом обработки персональных данных;
- основные подходы к системе управления процессом обработки персональных данных.

1.4. Положения настоящей Политики являются основой для организации работы по обработке персональных данных в Банке, в том числе, для разработки внутренних нормативных документов 2-го и 3-го уровня (регламентов, методик, технологических схем и пр.), регламентирующих процесс обработки персональных данных в Банке.

1.5. Положения настоящей Политики являются обязательными для исполнения всеми Работниками Банка, имеющими доступ к персональным данным.

1.6. Настоящая Политика размещается на общедоступном ресурсе - в ЭБВНД Банка для общего пользования Работниками Банка.

1.7. Ознакомление Работников Банка с положениями настоящей Политики осуществляется посредством рассылки Политики по системе электронного документооборота, используемого в Банке.

2. Цели обработки персональных данных

2.1. 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; об услугах дочерних обществ Банка; 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 Банку России;
- осуществления Банком Административно-хозяйственной деятельности;

а также для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей.

3. Классификация персональных данных и Субъектов персональных данных

3.1. 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.

3.2. 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.

3.3. Банк вправе осуществлять обработку специальной категории персональных данных, касающейся состояния здоровья Субъекта персональных данных (застрахованных лиц и иных лиц, в случаях предусмотренных действующим законодательством).

Банк вправе осуществлять обработку биометрических персональных данных с целью идентификации клиентов и работников Банка, при оказании банковских услуг и установления личности работников и посетителей при осуществлении пропуска на территорию Банка.

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

- физические лица, являющиеся Кандидатами;
- физические лица, являющиеся Работниками Банка и их близких родственников;
- физические лица, осуществляющие выполнение работ по оказанию услуг и заключившие с Банком договор гражданско-правового характера;
- физические лица, входящие в органы управления Банка;
- физические лица, представляющие интересы Корпоративного клиента Банка (Представители Корпоративного клиента);
- физические лица, являющиеся Розничными клиентами Банка;
- физические лица, приобретшие или намеревающиеся приобрести услуги Банка, услуги третьих лиц при посредничестве Банка или не имеющие с Банком договорных отношений при условии, что их персональные данные включены в автоматизированные системы Банка и обрабатываются в соответствии с Законодательством о персональных данных;
- физические лица, не относящиеся к Клиентам Банка, заключившие или намеревающиеся заключить с Банком договорные отношения в связи с осуществлением Банком Административно-хозяйственной деятельности при условии, что их персональные данные включены в автоматизированные системы Банка и обрабатываются в соответствии с Законодательством о персональных данных;
- 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.

4. Общие принципы обработки персональных данных

- 4.1. Банк осуществляет обработку персональных данных на основе общих принципов:
- 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.
- 4.2. В рамках обработки персональных данных для Субъекта персональных данных и Банка определены следующие права.
- 4.2.1. Субъект персональных данных имеет право:
- 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 случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении Субъектом персональных данных согласия на обработку персональных данных;
 - принимать предусмотренные законом меры по защите своих прав;
 - отозвать свое согласие на обработку персональных данных.
- 4.2.2. Банк имеет право:
- обрабатывать персональные данные Субъекта персональных данных в соответствии с заявленной целью;
 - требовать от Субъекта персональных данных предоставления достоверных персональных данных, необходимых для исполнения договора, оказания услуги, идентификации Субъекта персональных данных, а также в иных случаях, предусмотренных Законодательством о 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;
- поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных.

5. Основные участники системы управления процессом обработки персональных данных

5.1. В целях осуществления эффективного управления процессом обработки персональных данных определены основные его участники.

5.1.1. Правление Банка:

- определяет, рассматривает и утверждает политику Банка в отношении обработки персональных данных;
- назначает лиц (-о), ответственных (-ое) за организацию обработки персональных данных и определяет подразделение (-я), ответственное (-ые) за управление процессом обработки персональных данных.

5.1.2. Комитет ПАО Сбербанк по рискам группы:

- принимает решения по реализации действий Банка, связанных с использованием персональных данных, подверженных риску.

5.1.3. Лица (-о), ответственные (-ое) за организацию процесса обработки персональных данных¹:

- организует и контролирует разработку процесса обработки персональных данных (совершаемых с использованием средств автоматизации или без использования таких средств, в том числе на бумажных носителях) в соответствии с требованиями Законодательства о персональных данных и настоящей Политики;
- осуществляет управление процессом обработки персональных данных;
- разрабатывает и представляет для утверждения соответствующему коллегиальному органу Банка политику (-и) и локальные документы, касающиеся вопросов обработки персональных данных;
- осуществляет анализ, оценку и прогноз рисков, связанных с обработкой персональных данных в Банке;
- делегирует² иные функции, предусмотренные для лиц (-а), ответственных (-ого) за организацию обработки персональных данных, Законодательством о персональных данных, в профильные подразделения Банка.

5.1.4. Департамент безопасности:

¹ Лица (-о), ответственные (-ое) за организацию обработки персональных данных определяются (-ются) в соответствии с Реестром процессов ПАО Сбербанк. Реестр процессов ПАО Сбербанк размещен на корпоративном портале Банка. На момент утверждения настоящей Политики владельцами процессов обработки персональных данных определены руководители:

- Департамента развития отношений с клиентами и вторичных продаж (обработка персональных данных физических лиц, являющихся Розничными клиентами);
- Штаба блока «Корпоративный бизнес» (обработка персональных данных физических лиц, представляющих интересы Корпоративных клиентов Банка);
- Департамента HR-компетенций (обработка персональных данных физических лиц, являющихся Кандидатами, Работниками Банка, а также физических лиц, осуществляющих выполнение работ по оказанию услуг и заключивших с Банком договор гражданско-правового характера).

² Делегирование функций осуществляется в соответствии с организационно-распорядительными документами Банка.

- осуществляет разработку и организацию применения правовых, организационных и технических мер защиты персональных данных от неправомерного или случайного доступа к ним, Уничтожения, изменения, Блокирования, копирования, Предоставления, Распространения персональных данных, а также иных неправомерных действий в отношении персональных данных;
 - осуществляет определение угроз безопасности персональных данных при их обработке;
 - осуществляет оценку, обеспечение и контроль уровня защищенности информационных систем персональных данных;
 - осуществляет оценку эффективности принимаемых мер по обеспечению безопасности персональных данных;
 - осуществляет взаимодействие с органами государственной власти по вопросам защиты персональных данных;
 - осуществляет методологическую помощь подразделениям ЦА, ПЦП и территориальным банкам по вопросам взаимодействия с госорганами и регуляторами по вопросам обработки и защиты персональных данных;
 - разрабатывает внутренние процедуры, направленные на обеспечение безопасности и защиты персональных данных.

5.1.5. **Управление внутреннего аудита:**

- в рамках проводимых контрольных процедур оценивает эффективность системы внутреннего контроля Банка по обеспечению соблюдения требований настоящей Политики, а также утвержденных нормативных документов Банка в отношении персональных данных.

5.1.6. **Правовой департамент:**

- осуществляет мониторинг законодательства и доведение до сведения заинтересованных подразделений информации об изменении правовых норм;
- обеспечивает правовую защиту интересов Банка в судах и государственных органах по спорам, связанным с обработкой персональных данных, а также при рассмотрении административных дел, связанных с нарушением законодательства в указанной сфере.

6. Организация системы управления процессом обработки персональных данных

6.1. Обработка персональных данных Субъекта персональных данных осуществляется с его согласия на обработку персональных данных, а также без такового, если 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 или в иных случаях, предусмотренных Законодательством о персональных данных.

6.2. Обработка специальной категории персональных данных, касающейся состояния здоровья Субъекта персональных данных осуществляется с согласия Субъекта персональных данных на обработку своих персональных данных в письменной форме, а также без такового, если персональные данные сделаны общедоступными Субъектом персональных данных.

6.3. Банк вправе поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных, если иное не предусмотрено федеральным законом. Такая Обработка персональных данных осуществляется только на основании договора, заключенного между Банком и третьим лицом, в котором должны быть определены:

- перечень действий (операций) с персональными данными, которые будут совершаться третьим лицом, осуществляющим обработку персональных данных;
 - цели обработки персональных данных;
 - обязанности третьего лица соблюдать конфиденциальность персональных данных и обеспечивать их безопасность при обработке, а также требования к защите обрабатываемых персональных данных.
- 6.4. Банк осуществляет передачу персональных данных государственным органам в рамках их полномочий в соответствии с законодательством Российской Федерации.
- 6.5. Банк несет ответственность перед Субъектом персональных данных за действия лиц, которым Банк поручает обработку персональных данных Субъекта персональных данных.
- 6.6. Доступ к обрабатываемым персональным данным предоставляется только тем Работникам Банка, которым он необходим в связи с исполнением ими своих должностных обязанностей и с соблюдением принципов персональной ответственности.
- 6.7. Обработка персональных данных прекращается при достижении целей такой обработки, а также по истечении срока, предусмотренного законом, 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.
- 6.8. 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.
- 6.9. Банк обеспечивает конфиденциальность персональных данных Субъекта персональных данных со своей стороны, со стороны своих аффилированных лиц, со стороны своих Работников, имеющих доступ к персональным данным физических лиц, а также обеспечивает использование персональных данных вышеуказанными лицами исключительно в целях, соответствующих закону, договору или иному соглашению, заключенному с Субъектом персональных данных.
- 6.10. Обеспечение безопасности обрабатываемых персональных данных осуществляется Банком в рамках единой комплексной системы организационно-технических и правовых мероприятий по защите информации, составляющей банковскую и коммерческую тайну, с учетом требований Законодательства о персональных данных, принятых в соответствии с ним нормативных правовых актов. Система информационной безопасности Банка непрерывно развивается и совершенствуется на базе требований международных и национальных стандартов информационной безопасности, а также лучших мировых практик.

7. Заключительные положения

- 7.1. 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.
- 7.2. Политика является общедоступной и подлежит размещению на официальном сайте Банка или иным образом обеспечивается неограниченный доступ к настоящему документу.

Список терминов и определений

Административно-хозяйственная деятельность – внутрибанковские процессы, направленные на текущее обеспечение деятельности Банка товарно-материальными ценностями (осуществление закупок канцтоваров, офисного оборудования, расходных материалов, хозяйственных товаров, услуг связи и т.п.); на организацию документооборота (ведение архива, библиотек, баз данных); на организацию эксплуатации зданий, помещений, территорий (содержание, уборка, оформление и ремонт помещений); на организацию рабочего процесса.

Банк (оператор обработки персональных данных) – ПАО Сбербанк, осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, и действия, совершаемые с персональными данными.

Близкие родственники - являются родственники по прямой восходящей и нисходящей линии (родители и дети, дедушки, бабушки и внуки), полнородные и неполнородные (имеющие общих отца или мать) братья и сестры

Кандидат – физическое лицо, претендующее на вакантную должность в Банке, персональные данные которого приняты Банком.

Клиент – термин, используемый при совместном упоминании Корпоративного клиента и Розничного клиента.

Корпоративный клиент – юридическое лицо, индивидуальный предприниматель, а также физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, заключившее или намеревающееся заключить с Банком договор на оказание услуг.

Обработка персональных данных – любое действие (операция) Банка 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 (Предоставление, доступ), Обезличивание, Блокирование, удаление и Уничтожение персональных данных. В рамках Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» установлены следующие определения:

- Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
- 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.

Представитель Корпоративного клиента – физическое лицо, персональные данные которого переданы Банку и

- входящее в органы управления Корпоративного Клиента;

- являющееся владельцем/учредителем/акционером/участником Корпоративного клиента;
- действующее от имени Корпоративного клиента на основании доверенности/указанное в карточке с образцами подписей и оттиска печати Корпоративного клиента.

Работник Банка – физическое лицо, заключившее с Банком трудовой договор.

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

Розничный клиент – физическое лицо, которое заключило с Банком договор на оказание услуг, включая получение услуг путем присоединения к условиям публичного договора, и персональные данные которого переданы Банку.

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

- ПЦП** – подразделения центрального подчинения ПАО Сбербанк.
ЦА – Центральный аппарат ПАО Сбербанк.
ЭБВД – электронная база внутренних нормативных документов Банка.

ПРИЛОЖЕНИЕ 3.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННЫХ ДОКУМЕНТОВ

1. Конституция Российской Федерации.
2. Конвенция о защите физических лиц в отношении автоматизированной обработки данных личного характера (ETS N 108, заключена в г. Страсбурге 28.01.1981).
3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ с учетом изменений и дополнений.
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» с учетом изменений и дополнений.