«Согласовано»
Правлением ДБ АО «Сбербанк»
от «21» мая 2018 г.

«Утверждено»
Советом Директоров АБ АО «Сбербанк»
от «07» июня 2018 г.

Политика обработки персональных данных в ДБ АО «Сбербанк»

РЕЗЮМЕ ПО ВНД

Наименование ВНД	Политика обработки персональных данных в ДБ АО «Сбербанк»
Владелец ВНД	Департамент безопасности и защиты информации
Уровень доступа: «ВНД общего пользования», «Функциональный», «Конфиденциально»	ВНД общего пользования
Орган утверждения	Совет директоров ДБ АО «Сбербанк»
Мероприятия по ознакомлению структурных подразделений с ВНД	Рассылка по электронной почте в течение 3 (трех) рабочих дней с даты размещения ВНД в ЭББ на все структурные подразделения Банка
Ответственное лицо за доведение/обучение:	
на уровне ЦО:	Директор Департамента безопасности и защиты информации
на уровне филиалов:	Директора филиалов

Содержание

Глава 1. Общие положения

1. Настоящая Политика обработки персональных данных в ДБ АО «Сбербанк» (далее – Политика) разработана в соответствии с законодательством Республики Казахстан (далее - РК), Регламентом N 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/1/ЕС (Общий Регламент о защите персональных данных)" (принят в г. Брюсселе 27.04.2016) (далее - Регламент), и внутренними нормативными документами ДБ АО «Сбербанк» (далее - Банк).

2. Настоящая Политика разработана в целях реализации требований законодательства и международных документов 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.

3. Настоящая Политика устанавливает:

1) цели обработки персональных данных;

2) классификацию персональных данных и Субъектов персональных данных;

3) общие принципы обработки персональных данных;

4) основных участников системы управления процессом обработки персональных данных;

5) основные подходы к системе управления процессом обработки персональных данных.

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

5. **В настоящей Политике используются следующие понятия и определения:**

1) ***Банк*** – (оператор обработки персональных данных, контролер) – ДБ АО «Сбербанк», осуществляющий сбор, хранение, обработку, передачу, иные действия с персональными данными, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, и действия, совершаемые с персональными данными;

2) ***близкие родственники*** - в рамках настоящей политики супруг (супруга), родители (родитель), дети, усыновители (удочерители), усыновленные (удочеренные), полнородные и неполнородные братья и сестры, дедушка, бабушка, внуки;

3) ***ДБиЗИ*** – Департамент безопасности и защиты информации;

4) ***Кандидат*** - физическое лицо, претендующее на вакантную должность в Банке, персональные данные которого приняты Банком;

5) ***Клиент*** - термин, используемый при совместном упоминании Корпоративного клиента и Розничного клиента;

6) ***Корпоративный клиент*** - юридическое лицо, индивидуальный предприниматель, нотариус, адвокат, частный судебный исполнитель заключивший или намеревающейся заключить с Банком договор на оказание услуг, /оказывающий услуги/выполняющий работы для Банка;

7) ***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;

8) ***блокирование персональных данных*** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

9) ***обезличивание персональных данных*** - действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно;

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

11) ***уничтожение персональных данных*** - действия, в результате совершения которых невозможно восстановить персональные данные;

12) ***распространение персональных данных*** - действия, в результате совершения которых происходит передача персональных данных, в том числе через средства массовой информации или предоставление доступа к персональным данным каким-либо иным способом;

13) ***Реестр персональных данных*** – перечень, включающий в себя информацию о контролере, цели обработки, категориях персональных данных, категориях получателей персональных данных, сроки уничтожения, меры безопасности для защиты персональных данных;

14) ***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;

15) ***Субъект персональных данных*** - лицо, к которому относятся персональные данные.

Глава 2. Общие требования

6. Банк осуществляет обработку персональных данных в целях:

1) осуществления банковских и иных операций/услуг и сделок в соответствии с Уставом Банка и выданной Банку лицензией на совершение банковских и иных операций;

2) заключения с Субъектом персональных данных любых договоров и их дальнейшего исполнения;

3) проведения Банком акций, опросов, исследований;

4) 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;

5) ведения кадровой работы и организации учета работников Банка;

6) привлечения и отбора Кандидатов;

7) формирования статистической отчетности, в том числе для предоставления третьим лицам;

8) осуществления Банком административно-хозяйственной деятельности;

9) выявления случаев мошенничества, хищения денег со счета, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий;

10) иных целях.

Глава 3. Классификация персональных данных и Субъектов персональных данных

7. 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.

8. Банк не осуществляет обработку специальных категорий персональных данных, касающихся расовой и национальной принадлежности, политических взглядов,

религиозных и философских убеждений, интимной жизни, если иное не установлено законодательством РК.

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

10. 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.

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

1) физические лица, являющиеся Кандидатами;

2) физические лица, являющиеся Работниками Банка и их близких родственников;

3) физические лица, осуществляющие выполнение работ по оказанию услуг и заключившие с Банком договор гражданско-правового характера;

4) физические лица, входящие в органы управления Банка;

5) физические лица, представляющие интересы Корпоративного клиента Банка (Представители Корпоративного клиента);

6) физические лица, являющиеся Розничными клиентами Банка;

7) 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 РК;

8) 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 РК;

9) физические лица, персональные данные которых сделаны ими общедоступными, а их обработка не нарушает их прав и соответствует требованиям, установленным Законодательством РК;

10) иные физические лица, выразившие согласие на обработку Банком их персональных данных или физические лица, обработка персональных данных которых необходима Банку для достижения целей, предусмотренных Законом, для осуществления и выполнения возложенных законодательством РК на Банк функций, полномочий и обязанностей.

Глава 4. Общие принципы обработки персональных данных

12. Банк осуществляет обработку персональных данных на основе общих принципов:

1) обрабатываться законно, беспристрастно и прозрачным образом в отношении субъекта данных («законность, беспристрастность и прозрачность»);

2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных («целевое ограничение»);

3) соответствия объема, характера и способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных («минимизация данных»);

5) недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

6) хранения персональных данных в форме, позволяющей определить Субъекта персональных данных, не дольше, чем этого требуют цели их обработки («ограничение по хранению»);

7) уничтожения или обезличивания персональных данных по достижении целей их обработки, если срок хранения персональных данных не установлен законодательством РК, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных;

8) обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

9) обработки способом, гарантирующим соответствующую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки и от случайной потери, разрушения или уничтожения данных, с использованием соответствующих технических и организационных мер («целостность и конфиденциальность»);

10) точность и актуальность персональных данных; принятие обоснованных меры для того, чтобы гарантировать своевременное удаление или исправление неточных данных с учетом целей, для которых они обрабатываются («точность»).

13. Права Субъекта персональных данных в рамках обработки персональных данных:

1) знать о наличии у Банка, а также третьего лица своих персональных данных, а также получать информацию, содержащую:

подтверждение факта, цели, источников, способов сбора и обработки персональных данных;

перечень персональных данных;

сроки обработки персональных данных, в том числе сроки их хранения или если это не представляется возможным, критерии для определения указанного срока;

идентификационную информацию и контактные данные Банка и, при необходимости, его представителя;

контактные данные инспектора по защите персональных данных, в соответствующих случаях;

в соответствующих случаях, намерение Банка передать персональные данные третьей стране или международной организации;

о праве подачи жалобы в надзорный орган;

о том, является ли предоставление персональных данных требованием, предусмотренным законодательством или договором, или требованием, которое необходимо для заключения договора, а также обязан ли субъект данных предоставлять персональные данные и возможные последствия непредставления указанных данных;

о наличии автоматизированного процесса принятия решения, в том числе формирование профиля согласно и, как минимум в указанных случаях, достоверная информация о соответствующей логической схеме, а также о значимости и предполагаемых последствиях обработки для субъекта данных;

2) требовать от Банка изменения и дополнения своих персональных данных при наличии оснований, подтвержденных соответствующими документами;

3) требовать от Банка, а также третьего лица блокирования своих персональных данных в случае наличия информации о нарушении условий сбора, обработки персональных данных;

4) требовать от Банка, а также третьего лица уничтожения своих персональных данных, сбор и обработка которых произведены с нарушением законодательства РК, а также в иных случаях, установленных законодательством РК;

5) отозвать согласие на сбор, обработку персональных данных, кроме случаев, когда это противоречит законодательству РК или при наличии неисполненного обязательства;

6) дать согласие (отказать) Банку на распространение своих персональных данных в общедоступных источниках персональных данных;

7) на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда;

8) на осуществление иных прав, предусмотренных законодательством РК.

14. Права Банка в рамках обработки персональных данных:

1) обрабатывать персональные данные Субъекта персональных данных в соответствии с заявленной целью;

2) 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 РК;

3) 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 РК;

4) обрабатывать общедоступные персональные данные физических лиц;

5) осуществлять обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством РК;

6) поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных;

7) совершать иные действия, не противоречащие законодательству РК.

15. Банк должен обеспечить наличие копии обрабатываемых персональных данных. Если субъект данных подает запрос электронным способом, информация должна предоставляться в принятой электронной форме, если субъект данных не запрашивает иное.

Глава 5. Основные участники системы управления процессом обработки персональных данных

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

17. Правление Банка:

1) определяет, рассматривает и предварительно утверждает Политику обработки персональных данных;

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

18. Совет директоров Банка утверждает Политику обработки персональных данных.

19. Работник, ответственный за организацию обработки и защиту персональных данных, назначается приказом Председателя Правления Банка и выполняет следующие функции:

1) разрабатывает, организует и контролирует процесс обработки персональных данных (осуществляемый с использованием средств автоматизации или без использования таких средств, в том числе на бумажных носителях) в соответствии с Законодательством РК, настоящей Политикой, внутренними нормативными документами Банка;

2) осуществляет управление и постоянное совершенствование процесса обработки персональных данных по единым правилам, стандартизацию и тиражирование процесса;

3) разрабатывает и представляет для утверждения соответствующему коллегиальному органу Банка внутренние нормативные документы, касающиеся вопросов обработки персональных данных, требований к защите персональных данных;

4) организует доведение и (или) доводит до сведения работников Банка положений Законодательства РК, настоящей Политики, внутренних нормативных документов Банка по вопросам обработки персональных данных, требований к защите персональных данных;

5) осуществляет анализ, оценку и прогноз рисков, связанных с обработкой персональных данных в Банке, выработку мер по снижению рисков;

6) осуществляет оценку влияния процессов на права и свободы субъектов персональных данных;

7) осуществляет анализ автоматизированных систем и процессов обработки персональных данных на предмет соответствия установленным обязательным требованиям в области обработки и защиты персональных данных;

8) осуществляет ведение учета процедур и средств обработки персональных данных, в том числе Реестра персональных данных;

9) осуществляет контроль наличия и полноты содержания договоров поручения на обработку персональных данных, договоров на передачу персональных данных (DTA);

10) 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;

11) осуществляет определение угроз безопасности персональных данных при их обработке;

12) осуществляет организацию и контроль уровня защищенности информационных систем персональных данных;

13) осуществляет оценку эффективности принимаемых мер по обеспечению безопасности персональных данных;

14) разрабатывает внутренние процедуры, направленные на обеспечение безопасности и защиты персональных данных;

15) организует и осуществляет внутренний контроль за соблюдением оператором/контролером и его работниками Законодательства РК, настоящей Политики, внутренних нормативных документов Банка, требований к защите персональных данных;

16) организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов;

17) осуществляет методологическую помощь структурным подразделениям Банка по вопросам взаимодействия с органами государственной власти и надзорными органами по вопросам обработки персональных данных;

18) осуществляет взаимодействие с органами государственной власти по вопросам защиты персональных данных;

19) осуществляет уведомление надзорного органа в соответствии с применимыми требованиями о фактах утечки персональных данных;

20) организует оповещение субъектов персональных данных о фактах утечки их персональных данных;

21) делегирует иные функции, предусмотренные для лица, ответственного за организацию обработки персональных данных и защиту персональных данных, Законодательством РК, в профильные подразделения Банка.

20. Управление внутреннего аудита:

1) 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.

21. Юридическое управление:

1) осуществляет мониторинг законодательства РК и доведение до сведения заинтересованных подразделений информации об изменении правовых норм;

2) обеспечивает правовую защиту интересов Банка в судах и государственных органах по спорам, связанным с обработкой персональных данных, а также при рассмотрении административных дел и гражданских дел, связанных с нарушением законодательства в указанной сфере.

22. Владельцы процессов Банка обеспечивают своевременное информирование Работника, ответственного за организацию обработки и защиту персональных данных о необходимости внесения изменений в Реестр персональных данных.

23. Требования к форме и порядку актуализации Реестра персональных данных утверждаются внутренними нормативными документами Банка.

Глава 6. Организация системы управления процессом обработки персональных данных

24. Обработка персональных данных Субъекта персональных данных осуществляется с его согласия на сбор и обработку персональных данных или в иных случаях, предусмотренных законодательством РК.

25. 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.

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

1) перечень действий (операций) с персональными данными, которые будут совершаться третьим лицом, осуществляющим обработку персональных данных;

2) цели обработки персональных данных;

3) обязанности третьего лица соблюдать конфиденциальность персональных данных и обеспечивать их безопасность при обработке, а также требования к защите обрабатываемых персональных данных.

27. Банк осуществляет передачу персональных данных государственным органам в рамках их полномочий в соответствии с законодательством РК.

28. Банк несет ответственность перед Субъектом персональных данных за действия лиц, которым Банк поручает обработку персональных данных Субъекта персональных данных.

29. 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 минимальной достаточности.

30. Обработка персональных данных прекращается при достижении целей такой обработки, а также по истечении срока, предусмотренного законодательством РК. 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 РК.

31. 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 законодательству, договору или иному соглашению, заключенному с Субъектом персональных данных.

32. Обеспечение безопасности обрабатываемых персональных данных осуществляется Банком в рамках единой комплексной системы организационно-технических и правовых мероприятий по защите информации, составляющей банковскую, коммерческую тайну и иную, охраняемую законом тайну, с учетом требований законодательства РК 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.

Глава 7. Ответственность

33. Все работники Банка несут персональную ответственность за неисполнение, либо ненадлежащее исполнение положений настоящей Политики в соответствии с внутренними нормативными документами Банка.

Глава 8. Заключительные положения

34. Требования настоящей Политики распространяются на всех работников Банка (штатных, временных, работающих по контракту и т.п.), в том числе в отношениях с третьими лицами (подрядчики, аудиторы и т.п.), охватываемых областью действия системы управления информационной безопасностью, которые задействованы в процессах обработки информации Банка.

35. Все работники Банка несут гражданско-правовую, административную и иную ответственность, предусмотренную законодательством РК за несоблюдение принципов и условий обработки персональных данных физических лиц, а также за разглашение или незаконное использование персональных данных в соответствии с законодательством РК.

36. Изменения и дополнения вносятся в настоящую Политику по мере необходимости, а также в соответствии с требованиями законодательства РК и внутренних нормативных документов Банка.

37. Текущий контроль за соблюдением настоящей Политики возлагается на ДБиЗИ.

38. Общий контроль за соблюдением норм настоящей Политики возлагается на Правление Банка.