Коммерческий банк «Хлынов»
(акционерное общество)
(АО КБ «Хлынов»)

01.11.2017 № 123-П

г. Киров

УТВЕРЖДЕНА
протоколом совета директоров
АО КБ «Хлынов»
от 30 октября 2017 № 23

Политика обработки персональных данных АО КБ «Хлынов»
(редакция 2)

Содержание

1. Общие положения

1.1. Настоящая Политика обработки персональных данных АО КБ «Хлынов» (Далее – «Политика») определяет основные принципы, цели, условия и способы обработки персональных данных АО КБ «Хлынов», а также требования к защите персональных данных, обрабатываемых в АО КБ «Хлынов» (далее – «Банк»).

1.2. Настоящая Политика определяет принципы, порядок и условия обработки персональных данных работников Банка и иных лиц, чьи персональные данные обрабатываются Банком, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Настоящая Политика разработана и определяется в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Трудовой кодекс Российской Федерации;
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановление Правительства Российской Федерации от 06.07.2008 № 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 01.11.2012 № 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 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и

методов по обезличиванию персональных данных»;

- а также в соответствии с иными нормативными правовыми актами Российской Федерации и локальными актами уполномоченных органов государственной власти.

1.4. В целях реализации настоящей Политики в Банке разрабатываются следующие внутренние нормативные документы:

- Положение о персональных данных, обрабатываемых в АО КБ «Хлынов»;
- Перечень персональных данных, обрабатываемых в АО КБ «Хлынов»;
- Положение по организации и проведению работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных, используемых в АО КБ «Хлынов»;
- Положение о порядке хранения и учета материальных носителей персональных данных в АО КБ «Хлынов»;
- Порядок предоставления персональных данных работников третьим лицам по желанию работника;
- Порядок запроса персональных данных работников у третьих лиц;
- иные локальные нормативные акты и документы, регламентирующие порядок обработки персональных данных в Банке.

2. Понятие и состав персональных данных

2.1. Термин «Персональные данные» определяется Банком в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а именно:

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

2.2. В зависимости от субъекта персональных данных, Банк обрабатывает персональные данные следующих категорий субъектов персональных данных:

- персональные данные работника (потенциального работника) Банка - информация, необходимая Банку в связи с трудовыми отношениями и касающиеся конкретного работника (потенциального работника) Банка;
- персональные данные аффилированного лица, персональные данные руководителя, участника (акционера) или сотрудника юридического лица, являющегося аффилированным лицом по отношению к Банку - информация, необходимая Банку для отражения в отчетных документах о деятельности Банка в соответствии с требованиями федеральных законов, нормативных документов Банка России и иных нормативных правовых актов;

- персональные данные клиента (потенциального клиента, партнера, контрагента), а также персональные данные руководителя, участника (акционера) или сотрудника юридического лица, являющегося клиентом (потенциальным клиентом, партнером, контрагентом) Банка - информация, необходимая Банку для выполнения своих обязательств в рамках договорных отношений с клиентом и для выполнения требований законодательства Российской Федерации;
- персональные данные заёмщика, залогодателя, поручителя, принципала (потенциального заёмщика, залогодателя, поручителя, принципала), а также персональные данные руководителя, участника (акционера) или сотрудника юридического лица, являющегося заёмщиком, залогодателем, поручителем, принципалом (потенциальным заёмщиком, залогодателем, поручителем, принципалом) - информация, необходимая Банку для выполнения своих договорных обязательств и осуществления прав в рамках соответствующего договора, заключенного с заёмщиком, залогодателем, поручителем, принципалом, для минимизации рисков Банка, связанных с нарушением обязательств по кредитному договору (договору залога, договору поручительства, договору о предоставлении банковской гарантии) и для выполнения требований законодательства Российской Федерации.

3. Цели обработки персональных данных

Банк осуществляет обработку персональных данных в следующих целях:

- осуществления банковских операций и иной деятельности, предусмотренной Уставом и лицензиями Банка, нормативными актами Банка России, действующим законодательством Российской Федерации, в том числе Федеральными законами «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О страховании вкладов физических лиц в банках РФ», «Об индивидуальном (персонифицированном) учёте в системе обязательного пенсионного страхования», «О персональных данных», «Об акционерных обществах»;
- заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством и Уставом Банка;
- заключения, исполнения и прекращения трудовых договоров с физическими

лицами, организации кадрового учёта и ведения кадрового делопроизводства Банка, обеспечения соблюдения законов и иных нормативно-правовых актов; содействия работникам в трудоустройстве, обучении и продвижении по службе; обеспечения личной безопасности работников; контроля количества и качества выполняемой работы; обеспечения сохранности имущества.

4. Сроки обработки персональных данных

4.1. Сроки обработки персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, сроком исковой давности, приказом Минкультуры России от 25.08.2010 № 558 "Об утверждении "Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения", постановлением ФКЦБ РФ от 16.07.2003 № 03-33/пс "Об утверждении Положения о порядке и сроках хранения документов акционерных обществ", а также иными требованиями законодательства Российской Федерации и нормативными документами Банка России.

4.2. В Банке создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в Банке данных типовых форм документов установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5. Права и обязанности Банка

5.1. Банк как оператор персональных данных, вправе:

- отстаивать свои интересы в суде;
- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;
- использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством.

5.2. При обработке персональных данных Банк обязан принимать все меры для соблюдения прав субъектов персональных данных.

Субъект персональных данных имеет право:

- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать перечень своих персональных данных, обрабатываемых Банком и источник их получения;
- по своему заявлению разрешать Банку предоставлять свои персональные данные по запросам третьих лиц в случаях, когда закон не требует этого предоставления;
- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;
- определение своего представителя для защиты своих персональных данных;
- на доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;
- на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения.

6. Принципы и условия обработки персональных данных

6.1. Обработка персональных данных Банком осуществляется на основе принципов:

- законности и справедливости целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Банка;
- соответствия объёма и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки;

- недопустимости обработки избыточных по отношению к целям обработки персональных данных, а также обработки персональных данных сверх заявленных Банком при их сборе;
- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, но не дольше, чем этого требуют цели их обработки;
- уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

6.2. Обработка персональных данных осуществляется на основании условий, определенных законодательством Российской Федерации.

6.3. При заключении трудового договора с Банком субъект персональных данных дает согласие на обработку персональных данных по форме Приложения 1 к настоящей Политике. При необходимости обработки персональных данных для других целей форма согласия определяется в иных внутренних документах Банка.

7. Организация обработки персональных данных в Банке

7.1. Приказом председателя правления Банка назначается лицо, ответственное за организацию обработки персональных данных в Банке. Данное лицо получает указания непосредственно от председателя правления Банка и подотчетно председателю правления Банка.

7.2. Лицо, ответственное за организацию обработки персональных данных в Банке, обязано:

- осуществлять внутренний контроль за соблюдением Банком и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Банка положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовать приём и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

8. Обеспечение безопасности персональных данных

8.1. Обеспечение безопасности персональных данных является одной из приоритетных задач Банка.

8.2. Персональные данные являются конфиденциальной, строго охраняемой Банком информацией и на них распространяются все требования, установленные внутренними документами Банка к защите информации категории «Для служебного пользования».

8.3. Банк предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

8.4. Ответственность работников Банка, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных в Банке, определяется в соответствии с законодательством Российской Федерации и внутренними документами Банка.

9. Внутренний контроль

Внутренний контроль исполнения требований настоящей Политики и прочих локальных нормативных актов и документов, регламентирующих порядок обработки персональных данных в Банке, осуществляется с целью:

- обеспечения соответствия мероприятий по обработке Банком персональных данных, в том числе мероприятий по защите персональных данных, обязанностям, налагаемым на Банк Федеральными законами и локальными актами Президента и Правительства Российской Федерации, Банка России, ФСТЭК России, ФСБ России, Роскомнадзора; обеспечения соблюдения процедур и полномочий, установленных Федеральными законами и подзаконными локальными нормативными актами;
- достижения адекватности мер по обеспечению безопасности персональных данных при их обработке в Банке реальным угрозам информационной безопасности;
- повышения эффективности мероприятий по обеспечению обработки персональных данных, предотвращения или снижения ущерба Банку и/или субъектам персональных данных в случае нарушения установленных процессов обработки персональных данных в Банке.

Процесс определения, реализации, контроля и совершенствования мер информационной безопасности в банке содержит следующие критичные зоны регуляторного риска:

- соответствие мероприятий по обеспечению банком процедур обработки

персональных данных требованиям, установленным Федеральными законами и подзаконными локальными нормативными актами.

В целях снижения уровня правового, операционного, репутационного и регуляторного рисков в банке используется многоуровневая система внутреннего контроля:

9.1. Уровень №1. Предварительный контроль.

Все работники банка осуществляют на рабочих местах контроль исполнения требований настоящей Политики и прочих локальных нормативных актов и документов, регламентирующих порядок обработки персональных данных в Банке. О любых нарушениях установленных в Банке процедур обработки персональных данных, ставших известными работнику банка, работник обязан сообщить руководителю своего структурного подразделения, а также лицу, ответственному за организацию обработки персональных данных в Банке.

9.2. Уровень № 2. Текущий контроль.

Руководители структурных подразделений банка на постоянной основе контролируют исполнение работниками структурного подразделения требований настоящей Политики и прочих локальных нормативных актов и документов, регламентирующих порядок обработки персональных данных в Банке, осуществляют постоянный контроль порядка хранения носителей информации, составляющей персональные данные, не допускают до самостоятельной работы работников своего структурного подразделения, не прошедших обучение по вопросам безопасности обработки информации в Банке. О нарушениях или затруднениях в исполнении требований настоящей Политики и прочих локальных нормативных актов и документов, регламентирующих порядок обработки персональных данных в подразделении, руководитель структурного подразделения должен сообщить лицу, ответственному за организацию обработки персональных данных в Банке.

9.3. Уровень № 3. Дополнительный независимый контроль.

Лицо, ответственное за организацию обработки персональных данных в Банке, организует контроль исполнения требований настоящей Политики и прочих локальных нормативных актов и документов, регламентирующих порядок обработки персональных данных в Банке, на уровнях 1 и 2.

В целях, поставленных перед лицом, ответственным за организацию обработки персональных данных в Банке (в том числе для исполнения обязанностей, установленных настоящей Политикой), указанное лицо имеет право обращаться к руководителям

структурных подразделений с предложениями по повышению качества обработки персональных данных (в том числе безопасности обработки персональных данных и по вопросам качества внутреннего контроля в структурных подразделениях). Указанное лицо имеет право в разумные сроки получить от руководителей разъяснения по существу обращения.

Служба внутреннего контроля в рамках процедур управления регуляторным риском осуществляет контроль за соблюдением требований настоящей Политики и прочих локальных нормативных актов и документов, регламентирующих порядок обработки персональных данных в Банке, мониторинг и координацию мер, направленных на снижение уровня регуляторного риска. О случаях возникновения существенного регуляторного риска руководитель службы внутреннего контроля информирует председателя правления банка.

9.4. Уровень № 4. Контроль со стороны органов управления банком.

Председатель правления банка, на основании информации, поступающей с уровней №№ 1, 2 и 3 контроля, определяет меры по повышению эффективности внутреннего контроля исполнения требований настоящей Политики. Правление банка согласует меры по повышению эффективности процесса управления рисками, а также согласует внесение изменений в настоящую Политику, для последующего предоставления доработанной Политики на утверждение Совету директоров Банка.

9.5. Совет директоров АО КБ «Хлынов» на основании докладов руководителя службы внутреннего аудита принимает решения, направленные на улучшение качества процесса.

9.6. Контроль со стороны службы внутреннего аудита.

Служба внутреннего аудита производит периодический контроль соблюдения требований настоящей Политики и прочих локальных нормативных актов и документов, регламентирующих порядок обработки персональных данных в Банке, оценку системы внутреннего контроля, в том числе на наличие инструментов контроля, эффективности их использования соответствующими руководителями и должностными лицами АО КБ «Хлынов». Результаты оценки доводятся руководителем службы внутреннего аудита до Совета директоров АО КБ «Хлынов» для принятия решений, направленных на повышение эффективности системы внутреннего контроля, снижение банковских рисков на данном направлении деятельности АО КБ «Хлынов»».

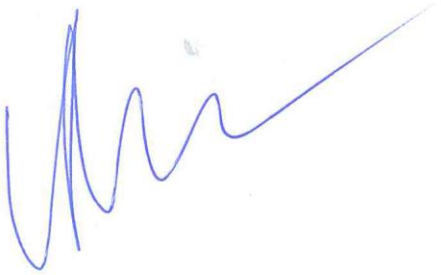
10. Заключительные положения

10.1. Настоящая Политика утверждается и вводится в действие протоколом заседания Совета директоров Коммерческого банка «Хлынов» (акционерное общество).

10.2. Решение о внесении изменений и дополнений в настоящую Политику принимается в порядке, предусмотренном пунктом 9.4.

10.3. Настоящая Политика является общедоступной и подлежит размещению на официальном сайте Банка.

10.4. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в пять лет.

Председатель правления Банка  И.П. Прозоров