Коммерческий банк «Хлынов»

(акционерное общество)

(АО КБ «Хлынов»)

23.09.2020 № 1-У

г. Киров

УТВЕРЖДЕНА
протоколом совета директоров
АО КБ «Хлынов»
от 17.09.2020 № 14

Политика АО КБ «Хлынов»
в отношении обработки персональных данных

Оглавление

1. Термины и определения

1.1. Сокращения, используемые в настоящей «Политике АО КБ «Хлынов» в отношении обработки персональных данных» (далее – Политика) имеют следующее значение:

ВНД – внутренний нормативный документ.

ПДн – персональные данные.

1.2. Термины, используемые в Политике равноприменимы в единственном и множественном числе и имеют следующие определения:

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Банк – коммерческий банк «Хлынов» (акционерное общество) (сокращённое наименование – АО КБ «Хлынов»), осуществляющий обработку ПДн, а также определяющий цели обработки ПДн, состав ПДн, подлежащих обработке, и действия, совершаемые с ПДн.

Близкие родственники – супруг, супруга, родители, дети, усыновители, усыновленные, дедушка, бабушка, внуки, полнородные и неполнородные (имеющих общего отца или мать) братья и сестры.

Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Доступ к ПДн – возможность получения ПДн и их использование.

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

Информационный актив – информация с реквизитами, позволяющими её идентифицировать; имеющая ценность для Банка; находящаяся в распоряжении Банка и представленная на любом материальном носителе в пригодной для её обработки, хранения или передачи форме.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Использование ПДн – действия (операции) с ПДн, совершаемые уполномоченным лицом в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

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

Клиент – при совместном упоминании **Розничный клиент** (физическое лицо, которое заключило с Банком договор на оказание услуг и ПДн которого переданы Банку) и

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

Конфиденциальная информация (сведения конфиденциального характера) – сведения, содержащие информацию, составляющую коммерческую, банковскую тайну Банка, информацию, являющуюся информацией «Для служебного пользования» и инсайдерскую информацию.

Конфиденциальность информационных активов – свойство информационной безопасности банковской системы Российской Федерации, состоящее в том, что обработка, хранение и передача информационных активов осуществляются таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.

Внутренний нормативный документ (ВНД) – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, создаваемая в Банке и используемая в его деятельности. Приложения к внутреннему документу являются его неотъемлемой частью.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение

(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

ПДн – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн).

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Работники – физические лица, вступившие в трудовые отношения с Банком.

Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Субъект ПДн – физическое лицо, которое прямо или косвенно определено, или определяемо с помощью ПДн.

Трансграничная передача ПДн – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угроза информационной безопасности ПДн – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия при их обработке в информационной системе ПДн или без использования средств автоматизации.

Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

2. Общие положения

2.1. Настоящая Политика определяет принципы, условия и способы обработки ПДн, в том числе защиты ПДн в Банке.

2.2. Настоящая Политика разработана в целях обеспечения необходимого и достаточного уровня информационной безопасности ПДн и процессов, связанных с их обработкой, а также для обеспечения защиты прав и свобод субъектов ПДн при обработке их ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2.3. В Банке обработка и обеспечение безопасности ПДн осуществляется в соответствии с законодательством Российской Федерации, внутренними нормативными документами Банка в области ПДн, в том числе требованиями к защите ПДн.

2.4. ПДн являются конфиденциальной, строго охраняемой информацией. На них распространяются все требования, установленные внутренними документами Банка к защите конфиденциальной информации.

2.5. С момента вступления в силу настоящей Политики считать утратившей силу «Политику обработки персональных данных АО КБ «Хлынов» (редакция 3), утвержденную протоколом совета директоров № 11 от 25.04.2019.

2.6. Политика обработки ПДН разработана и определяется в соответствии с:

2.6.1. Конституцией Российской Федерации;

2.6.2. Трудовым кодекс Российской Федерации;

2.6.3. Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее – Закон о персональных данных);

2.6.4. Указом Президента Российской Федерации от 06 марта 1997 г. №188 «Об утверждении Перечня сведений конфиденциального характера»;

2.6.5. Постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

2.6.6. Постановлением 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»;

2.6.7. Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2.6.8. Приказом 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».

2.6.9. Приказом Роскомнадзора от 05 сентября 2013 г. №996 «Об утверждении требований и методов по обезличиванию персональных данных»;

2.6.10. Иными нормативными правовыми актами, касающимися обработки ПДн (в том числе изданные государственными органами, Банком России, органами местного самоуправления в пределах своих полномочий).

2.6.2. Положения настоящей Политики являются основой для организации работы по обработке ПДн в Банке, в том числе, для разработки ВНД 2-го и 3- го уровня (регламентов,

положений, методик, технологических схем и пр.), регламентирующих процесс обработки ПДн в Банке.

3. Цели обработки ПДн

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;
- регулирования трудовых и иных, непосредственно связанных с ними отношений;
- выявления случаев мошенничества, хищения денежных средств со счета, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий;

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.

4. Принципы и условия обработки ПДн в Банке

4.1. В Банке соблюдаются следующие принципы обработки ПДн:

4.1.1. Обработка ПДн осуществляется в соответствии с конкретными заранее определенными и законными целями и производится только до момента достижения этих целей.

4.1.2. Содержание и объем ПДн не противоречат заявленным целям, не являются избыточными по отношению к ним.

4.1.3. При обработке ПДн в Банке обеспечиваются точность, достаточность, актуальность ПДн по отношению к целям обработки за счет применения необходимых мер по удалению или уточнению неполных, или неточных данных.

4.1.4. Объединение баз данных, содержащих ПДн, цели обработки которых не совместимы между собой, недопустимо.

4.1.5. Хранение ПДн осуществляется в форме, позволяющей идентифицировать субъект ПДн, и ограничивается установленными целями обработки ПДн.

4.1.6. По достижении целей обработки или в случае утраты необходимости их достижения ПДн подлежат уничтожению в соответствии с законодательством.

4.2. В Банке соблюдаются следующие условия обработки ПДн:

4.2.1. Обработка ПДн в Банке осуществляется только с согласия субъекта ПДн на обработку его ПДн, если иное не предусмотрено законодательством.

4.2.2. Банк вправе поручить обработку ПДн третьему лицу, в том числе находящемуся за пределами Российской Федерации (трансграничная передача) с согласия субъекта ПДн на основании заключаемого с этим лицом договора при обязательном включении в него перечня действий с ПДн, целей их обработки, требований к их защите, обязанностей третьего лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке. В случае трансграничной передачи данных Банк помимо прочего обязан убедиться в том, что третьим лицом обеспечивается адекватная защита прав субъектов ПДн до начала осуществления такой передачи. Если адекватная защита не может быть обеспечена, то трансграничная передача ПДн может осуществляться только при наличии соответствующего согласия в письменной форме субъекта ПДн или в случаях, установленных п.2-5 ч.4 ст.12 Закона о персональных данных.

4.2.3. Банк несет ответственность перед субъектом ПДн за обработку ПДн, в том числе выполняемую третьим лицом на основании договора.

4.2.4. Работники Банка, имеющие доступ к ПДн, не раскрывают ПДн третьим лицам и не распространяют их без согласия субъекта ПДн, если иное не предусмотрено законодательством.

5. Перечень субъектов, ПДн которых обрабатываются в Банке

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);
- посетители, в т.ч. информационных ресурсов Банка;
- 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.

6. Перечень ПДн, обрабатываемых в Банке

6.1. Перечень ПДн, обрабатываемых Банком, определяется в соответствии с законодательством Российской Федерации и ВНД Банка с учетом целей обработки ПДн, указанных в разделе 3 настоящей Политики.

6.2. 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. Данные сведения предусматривают обработку при наличии согласия субъекта ПДн за исключением случаев, указанных в ч.2 ст. 11 Закона о персональных данных (к числу биометрических ПДн, не требующих согласия субъекта ПДн на обработку, среди прочего могут быть отнесены записи внутренних систем охранного телевидения).

6.3. 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.

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

7. Способы обработки ПДн

7.1. Банк осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление и уничтожение ПДн.

7.2. Обработка ПДн в Банке осуществляется следующими способами:

7.2.1. без использования средств автоматизации;

7.2.2. с использование средств автоматизации с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

7.2.3. смешанная обработка ПДн.

8. Права субъекта ПДн

8.1. В установленном законодательством РФ порядке субъект ПДн вправе получать доступ к следующим сведениям:

8.1.1. Подтверждение факта обработки ПДн Банком.

8.1.2. Правовые основания и цели обработки ПДн.

8.1.3. Цели и применяемые Банком способы обработки ПДн.

8.1.4. Наименование и место нахождения оператора, сведения о лицах (за исключением работников Банка), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Банком или на основании Федерального закона.

8.1.5. Обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом.

8.1.6. Сроки обработки ПДн, в том числе сроки их хранения.

8.1.7. Порядок реализации субъектом ПДн прав, предусмотренных Законом о персональных данных.

8.1.8. Информация об осуществленной или о предполагаемой трансграничной передаче ПДн.

8.1.9. Наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу.

8.1.10. Иные сведения, предусмотренные Законом о персональных данных или другими Федеральными законами.

8.2. Субъект ПДн имеет право на:

8.2.1. Принятие предусмотренных законом мер по защите своих прав.

8.2.2. Уточнение, блокирование или уничтожение его ПДн в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или избыточными по отношению к заявленной цели обработки.

8.2.3. Получение сведений, указанных в п. 8.1. настоящей Политики, в полном объеме, а также ознакомление с обрабатываемыми ПДн при направлении запроса или обращения в Банк.

8.2.4. Повторное обращение или запрос на предоставление информации об обрабатываемых ПДн в случае, если они не были предоставлены в полном объеме относительно первоначального запроса.

8.2.5. Обжалование действия или бездействия Банка в уполномоченный орган в случае осуществления Банком обработки ПДн субъекта с нарушением требований законодательства, а также прав и свобод субъекта ПДн, в судебном порядке.

8.2.6. Компенсацию морального вреда независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков и возмещение убытков в судебном порядке.

9. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Законом о персональных данных

9.1. Банк при осуществлении обработки ПДн:

9.1.1. Назначает лицо, ответственное за организацию обработки ПДн в Банке, которое доводит до работников Банка положения законодательства Российской Федерации и ВНД Банка в области ПДн и осуществляет внутренний контроль за их соблюдением.

9.1.2. Применяет правовые, организационные и технические меры для защиты ПДн от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

9.1.3. Издает ВНД, определяющие политику и вопросы обработки и защиты ПДн в Банке, а также устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

9.1.4. Проводит оценку вреда, который может быть причинен Субъектам ПДн в случае нарушения действующего законодательства, соотносит указанный вред и принимаемые оператором меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных.

9.1.5. Осуществляет ознакомление работников Банка, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации и ВНД Банка в области ПДн, в том числе требованиями к защите ПДн, и проводит обучение указанных работников.

9.1.6. Публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике.

9.1.7. Осуществляет сбор ПДн субъекта с соблюдением требований, предусмотренных ст.18 Закона о персональных данных с предоставлением субъекту ПДн информации, указанной в п. 8.1. настоящей Политики, а в случае получения ПДн не от субъекта ПДн информацию в соответствии с ч.4 ст.18 Закона о персональных данных и в случае отказа от предоставления ПДн, которые должны быть предоставлены на основании Федерального закона, разъясняет субъекту ПДн последствия этого отказа.

9.1.8. При обращении либо получении запроса субъекта ПДн или его законного представителя на доступ к ПДн Банк предоставляет ему сведения, указанные в п. 8.1.

настоящей Политики, в доступной форме, не раскрывая при этом ПДн, относящихся к другим субъектам ПДн, за исключением случаев наличия законного основания.

9.1.9. Устраняет нарушения законодательства, допущенные при обработке ПДн, в установленном порядке.

9.1.10. Прекращает обработку и уничтожает ПДн в случаях, предусмотренных законодательством Российской Федерации в области ПДн.

9.1.11. Совершает иные действия, предусмотренные законодательством Российской Федерации в области ПДн.

10. Меры, принимаемые Банком для обеспечения безопасности ПДн

10.1. В Банке реализуются следующие необходимые и достаточные меры по защите ПДн:

10.1.1. Назначение лица, ответственного за организацию обработки ПДн.

10.1.2. Распределение обязанностей и установление персональной ответственности лиц, осуществляющих обработку ПДн, за нарушение правил обработки ПДн, установленных ВНД Банка и законодательством Российской Федерации.

10.1.3. Принятие ВНД и иных документов в области обработки и защиты ПДн.

10.1.4. Обособление ПДн, обрабатываемых без использования средств автоматизации, от иной информации, в частности путем их фиксации на отдельных материальных носителях ПДн, в специальных разделах.

10.1.5. Исключение объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

10.1.6. Осуществление внутреннего контроля соответствия обработки Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, настоящей Политике, ВНД Банка.

10.1.7. Организация пропускного режима в помещениях, в которых обрабатываются ПДн.

10.1.8. Организация работы с документами и материальными носителями, содержащими ПДн.

10.1.9. Реализация необходимых организационных и технических мер для обеспечения безопасности ПДн от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

10.1.10. Назначение ответственного за организацию обработки ПДн в Банке в целях координации действий по обеспечению безопасности ПДн.

10.1.11. Контроль за реализацией требований информационной безопасности при обработке ПДн.

10.1.12. Иные меры по обеспечению безопасности обрабатываемых в Банке ПДн.

11. Контроль за соблюдением законодательства Российской Федерации и ВНД Банка в области ПДн

11.1. Организация и осуществление внутреннего контроля за соблюдением подразделениями Банка законодательства Российской Федерации и ВНД Банка в области ПДн, в том числе требований к защите ПДн, обеспечиваются лицом, ответственным за организацию обработки ПДн в Банке.

11.2. Внутренний контроль соответствия обработки ПДн Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, настоящей Политике, ВНД Банка осуществляет отдел информационной безопасности Банка.

11.3. Ответственность за соблюдение требований законодательства Российской Федерации и ВНД Банка в области ПДн, а также за обеспечение конфиденциальности и безопасности ПДн в подразделениях Банка возлагается на их руководителей.

12. Заключительные положения

12.1. Настоящая Политика подлежит размещению на официальном сайте Банка в информационно-телекоммуникационной сети «Интернет» по адресу: https://www.bank-hlynov.ru/.

12.2. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки ПДн Банка.

12.3. Ответственность должностных лиц Банка, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн, определяется в соответствии с законодательством Российской Федерации и внутренними документами Банка.

12.4. Пересмотр настоящей Политики должен производиться в случае изменения законодательства в области ПДн и специальных нормативных документов по обработке и защите ПДн, изменения бизнес-процессов Банка, требующих изменения перечня обрабатываемых ПДн, а также по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности банковских информационных технологических процессов, но не реже одного раза в три года.

12.5. Ответственным за актуализацию Политики является отдел информационной безопасности Банка.

Начальник ОИБ Е.А. Карпов

Председатель правления Банка И.П. Прозоров