Утверждаю:
Председатель Совета
ПАО Комбанк «Химик»
Протокол № 15 от 07.12.2018 г.

Политика
обработки персональных данных
в Публичном акционерном обществе
коммерческий банк
«Химик»

Дзержинск
2018

1. Общие положения.

1.1. Настоящая Политика об обработке персональных данных в Публичном акционерном обществе коммерческий банк «Химик» (далее – Политика):

- Является основополагающим внутренним документом Публичного акционерного общества коммерческий банк «Химик» (далее – Банк»), регулирующим вопросы обработки персональных данных в Банке;
- Разработана в целях обеспечения реализации требований законодательства РФ в области обработки персональных данных, направленного на обеспечение 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, в частности в целях защиты от несанкционированного доступа и неправомерного распространения персональных данных, обрабатываемых в Банке;
- Раскрывает основные категории персональных данных, обрабатываемых Банком, цели, способы и принципы обработки Банком персональных данных, права и обязанности Банка при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых Банком в целях обеспечения безопасности персональных данных при их обработке;
- Предназначена для работников Банка, осуществляющих обработку персональных данных в целях непосредственной реализации ими закрепленных в Политике принципов, а также является информационным ресурсом для субъектов персональных данных, позволяющим определить концептуальные основы деятельности Банка при обработке персональных данных.

2. Источники нормативного правового регулирования вопросов обработки персональных данных.

2.1. Политика Банка в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 02.12.1990 №395-1 «О банках и банковской деятельности»;
- Указ Президента РФ 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 01.12.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах 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 Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора)

за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных».

- Стандарт Банка России СТО БР ИББС «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

2.2. Во исполнение настоящей Политики в Банке приказами Председателя Правления утверждаются следующие локальные нормативные правовые акты:

- Положение об обработке персональных данных в Публичном акционерном обществе коммерческий банк «Химик»;
- Перечень обрабатываемых персональных данных в ПАО Комбанк «Химик»;
- Положение о порядке отнесения автоматизированных банковских систем Публичного акционерного общества коммерческий банк «Химик» к информационным системам персональных данных;
- Перечень информационных систем персональных данных в ПАО Комбанк «Химик»;
- Перечень подразделений и сотрудников, допущенных к работе с персональными данными в ПАО Комбанк «Химик»;
- Модель угроз и нарушителей информационной безопасности ПАО Комбанк «Химик»;
- Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «1С:Предприятие» ПАО Комбанк «Химик»;
- Инструкция администратора ИСПДн ПАО Комбанк «Химик»;
- Инструкция администратора безопасности при использовании ресурсов объекта вычислительной техники ПАО Комбанк «Химик»;
- Акты и заключения о классификации информационных систем персональных данных ПАО Комбанк «Химик»;
- Иные локальные документы Банка, принимаемые во исполнение требований действующих нормативных правовых актов РФ в области персональных данных.

3. Основные термины и понятия, используемые в локальных документах Банка, принимаемых по вопросу обработки персональных данных.

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

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на

ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

Материальный носитель персональных данных – материальный объект, используемый для закрепления и хранения информации. В целях настоящей Политики под материальным носителем понимается бумажный документ, диск, дискета, флеш-карта и т.п.

Цель обработки персональных данных – конкретный конечный результат действий, совершенных с персональными данными, соответствующий требованиям законодательства РФ и направленный в том числе на создание необходимых правовых условий для достижения оптимального согласования интересов сторон.

4. Общие условия обработки Банком персональных данных.

4.1. Обработка персональных данных осуществляется в Банке на основе следующих принципов:

4.1.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

4.1.2. Обработка персональных данных должна быть ограничена достижением конкретных, заранее определенных и законных целей.

4.1.3. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.1.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.1.5. Допускается обработка исключительно тех персональных данных, которые отвечают целям их обработки.

4.1.6. Содержание и объем персональных данных должны соответствовать заявленным целям обработки.

4.1.7. Не допускается обработка персональных данных, излишних по отношению к заявленным целям обработки.

4.1.8. При обработке персональных данных должна быть обеспечена точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

4.1.9. Неполные или неточные данные должны быть удалены или уточнены.

4.1.10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

4.1.11. По достижении целей обработки или в случае утраты необходимости в достижении этих целей, персональные данные должны быть уничтожены или обезличены, если иное не предусмотрено федеральным законом.

4.2. Банк при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.3. Обеспечение безопасности персональных данных достигается, в частности:

4.3.1. Определением угроз персональных данных при их обработке в информационных системах персональных данных;

4.3.2. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

4.3.3. Применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

4.3.4. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

4.3.5. Учет машинных носителей персональных данных;

4.3.6. Обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

4.3.7. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4.3.8. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

4.3.9. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4.4. Перечень персональных данных, обрабатываемых в Банке утверждается Председателем Правления и по мере изменения состава обрабатываемых персональных данных подлежит пересмотру и уточнению.

4.5. Субъектами персональных данных, обработка которых осуществляется Банком, являются:

- Работники Банка;
- Акционеры Банка;
- Правопреемники акционеров Банка;
- Представители акционеров Банка;
- Физические лица – клиенты Банка;
- Правопреемники физических лиц – клиентов Банка;
- Представители физических лиц – клиентов Банка;
- Руководители юридических лиц – клиентов Банка;
- Представители юридических лиц – клиентов Банка;
- Физические лица, заключившие с Банком договоры гражданско-правового характера;
- Члены органов управления и контроля за деятельностью Банка..

4.6. Цели обработки персональных данных:

4.6.1. Осуществление возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: "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 Российской Федерации", "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования", "О персональных данных", нормативными актами Банка России, а также Уставом и нормативными актами ПАО Комбанк «Химик»;

4.6.2. Организация учета служащих Банка для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия служащему в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: "Об индивидуальном

(персонифицированном) учете в системе обязательного пенсионного страхования", "О персональных данных", а также Уставом и нормативными актами ПАО Комбанк «Химик».

4.7. При определении объема и содержания обрабатываемых данных субъектов, Банк руководствуется указанными целями получения и обработки персональных данных.

4.8. Доступ работников Банка к персональным данным, подлежащим обработке, разрешен только уполномоченным сотрудникам в соответствии с Перечнем сотрудников, допущенных к работе с персональными данными в ПАО Комбанк «Химик». При этом указанным лицам предоставляется доступ только к персональным данным, необходимым для выполнения их служебных обязанностей в пределах задач и функций их подразделений.

4.9. Порядок доступа субъектов персональных данных к его персональным данным, обрабатываемых Банком, осуществляется в соответствии с Федеральным законом №152-ФЗ «О персональных данных» и определяется Положением об обработке персональных данных в ПАО Комбанк «Химик».

4.10. Перечень информационных систем персональных данных ПАО Комбанк «Химик» утверждается Председателем Правления. Информационные системы персональных данных классифицируются в зависимости от категорий обрабатываемых в них персональных данных.

4.11. Организация и проведение мероприятий по обеспечению защиты персональных данных в Банке осуществляется в соответствии с Положением об обработке персональных данных в ПАО Комбанк «Химик».

4.12. Общее руководство организацией работ по защите персональных данных в Банке осуществляет ответственный сотрудник за обеспечение безопасности персональных данных.

4.13. Для выбора и обоснования мер защиты, их уточнения и контроля за их исполнением, в Банке создана Комиссия по обеспечению выполнения законодательных требований при обработке персональных данных.

4.14. Деятельность Банка по обеспечению безопасности персональных данных контролируется уполномоченным органом по защите прав субъектов персональных данных.