АКЦИОНЕРНОЕ ОБЩЕСТВО
КОММЕРЧЕСКИЙ БАНК «МОДУЛЬБАНК»

УТВЕРЖДЕНО
Правлением
АО КБ «Модульбанк»

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в АО КБ «Модульбанк»

Кострома, 2017

1. Назначение и область действия документа

1.1. Положение АО КБ «Модульбанк» (далее – Банк) об обработке и защите персональных данных (далее – Положение) определяет позицию и намерения Банка в области обработки и реализации требований к защите персональных данных лиц, состоящих в договорных, гражданско-правовых и иных отношениях с Банком, соблюдения действующего законодательства Российской Федерации в области информационной безопасности, а также требований Федерального закона от 27.06.2006 года №152-ФЗ «О персональных данных», основной целью которого является 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.

1.2. Положение предназначено для изучения и неукоснительного исполнения всеми сотрудниками Банка, а также подлежит доведению до сведения лиц, состоящих в договорных, гражданско-правовых и иных отношениях с Банком (далее – граждане), партнеров и других заинтересованных сторон.

2. Определения

2.1. Под персональными данными (далее – ПДн) понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (гражданину).

2.2. Под обработкой ПДн понимается любое действие (операция) или совокупность действий (операций) с ПДн, совершаемых с использованием средств автоматизации или без использования таких средств. К таким действиям (операциям) можно отнести: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

3. Основные положения

3.1. Понимая важность и ценность информации о человеке, Банк обеспечивает надежную защиту предоставленных ПДн. Банк обрабатывает ПДн только тех лиц, которые состоят в договорных, гражданско-правовых и иных отношениях с Банком, а именно:

- лиц, состоящих в трудовых отношениях с Банком (сотрудники Банка);

- лиц, являющихся соискателями должностей в Банке;

- лиц, являющихся Клиентами или Партнерами Банка.

3.2. Под безопасностью ПДн Банк понимает защищенность ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн и принимает необходимые правовые, организационные и технические меры для защиты ПДн.

3.3. Обработка ПДн сотрудников Банка осуществляется в строгом соответствии с трудовым законодательством РФ. Данные клиентов Банка, полученные в связи с заключением договора, стороной которого является субъект ПДн, обрабатываются с соблюдением принципов и условий обработки ПДн, установленных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон «О персональных данных»). Банк не осуществляет распространение или раскрытие ПДн без согласия гражданина, если иное не предусмотрено федеральным законом.

3.4. Правовым основанием обработки ПДн является осуществление возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, Федеральными законами, в частности: «О банках и банковской деятельности» № 395-1 от 02.12.1990 г., «О Центральном банке Российской Федерации (Банке России)» № 86-ФЗ от 10.07.2002 г., «О национальной платежной системе» № 161-ФЗ от 27.06.2011 г., «О кредитных историях» № 218-ФЗ от 30.12.2004 г., «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» № 115-ФЗ от 07.08.2001 г., «О валютном регулировании и валютном контроле» № 173-ФЗ от 10.12.2003 г., «О рынке ценных бумаг» № 39-ФЗ от 22.04.1996 г., «О несостоятельности (банкротстве) кредитных организаций» № 40-ФЗ от 25.02.1999 г., «О страховании вкладов физических лиц в банках Российской Федерации» № 177-ФЗ от 23.12.2003 г., «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» № 27-ФЗ от 01.04.1996 г., «О персональных данных» № 152-ФЗ от 27.07.2006 г., «Об акционерных обществах» № 208-ФЗ от 26.12.1995, «Об электронной подписи» № 63-ФЗ от 06.04.2011 г., принятыми в их исполнение нормативными актами Банка России, а также в целях организации учета служащих кредитной организации 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 нормативными актами Банка России.

3.5. При обработке ПДн Банк придерживается следующих принципов:

- Банк осуществляет обработку ПДн только на законной и справедливой основе;

- обработка ПДн в Банке ограничивается достижением конкретных, заранее определенных и законных целей;

- в Банке не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

- до начала сбора/получения ПДн, Банк определяет конкретные законные цели обработки ПДн;

- Банк собирает только те ПДн, которые являются необходимыми и достаточными для заявленной цели обработки;

- Банк систематически принимает меры по удалению или уточнению неполных или неточных данных;

- Банк уничтожает либо обезличивает ПДн по достижении целей обработки или в случае утраты необходимости в достижении целей[1];

- Банк не раскрывает третьим лицам и не распространяет персональные данные без согласия гражданина (если иное не предусмотрено действующим законодательством Российской Федерации);

- Банк не осуществляет сбор и обработку персональных данных граждан, касающихся расовой, национальной принадлежности, политических, религиозных, философских и иных убеждений, состояния здоровья, интимной жизни, членства в общественных объединениях, в том числе в профессиональных союзах.

3.6. Банк вправе поручить обработку персональных данных (с согласия гражданина[2]) юридическому лицу, на основании заключаемого с этим лицом договора, в котором указанные лица обязуются соблюдать принципы и правила обработки персональных данных, предусмотренные Законом «О персональных данных». В договоре (поручении Банка) должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность ПДн при их обработке.

3.7. В случае осуществления Банком трансграничной передачи ПДн граждан на территорию иностранного государства, указанная трансграничная передача должна осуществляться с соблюдением требований действующего законодательства Российской Федерации, а также международно-правовых актов. При этом получающей стороной могут быть страны, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, а также иные иностранные государства при условии обеспечения адекватных защитных мер прав субъектов ПДн.

4. Права граждан в части обработки персональных данных

4.1. Гражданин, ПДн которого обрабатываются в Банке имеет право:

- требовать от Банка уточнения его ПДн их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- отозвать свое согласие на обработку ПДн;

- требовать устранения неправомерных действий Банка в отношении его ПДн;

- обжаловать действия или бездействие Банка в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если гражданин считает, что Банк осуществляет обработку его ПДн с нарушением требований Закона «О персональных данных» или иным образом нарушает его права и свободы;

---

[1] Если иное не предусмотрено соглашением между Банком и гражданином либо если Банк не вправе осуществлять обработку ПДн без согласия гражданина на основаниях, предусмотренных Законом «О персональных данных» или другими федеральными законами.

[2] Если иное не предусмотрено федеральным законом.

- обжаловать действия или бездействие Банка в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если гражданин считает, что Банк осуществляет обработку его ПДн с нарушением требований Закона «О персональных данных» или иным образом нарушает его права и свободы;

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

4.2. Гражданин имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Банком;

- правовые основания и цели обработки ПДн;

- сведения о применяемых Банком способах обработки ПДн;

- наименование и место нахождения Банка;

- 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;

- перечень обрабатываемых ПДн, относящихся к гражданину, от которого поступил запрос и источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

- сроки обработки ПДн, в том числе сроки их хранения;

- порядок осуществления гражданином прав, предусмотренных Законом «О персональных данных»;

- информацию об осуществляемой или о предполагаемой трансграничной передаче ПДн;

- наименование (Ф.И.О.) и адрес лица, осуществляющего обработку ПДн по поручению Банка;

- иные сведения, предусмотренные Законом «О персональных данных» или другими федеральными законами.

5. Внесение изменений в Положение

5.1. Настоящее Положение подлежит изменению по мере необходимости, но не реже чем 1 раз в 3-и года, а также:

- при изменении законодательства Российской Федерации в области ПДн;

- при изменении состава лиц, которым Банк поручает обработку ПДн;

- в случаях выявления несоответствий, затрагивающих обработку ПДн;

- по результатам контроля выполнения требований по обработке и защите ПДн;

- по решению руководства Банка.

5.2. Актуальная версия настоящего Положения публикуется на официальном сайте Банка – https://www.modulbank.ru.

6. Ответственность

6.1. Ответственным за организацию процесса обработки персональных данных Приказом по Банку назначается сотрудник Операционного блока Банка.

6.2. Ответственным за организацию технических мероприятий по созданию системы защиты персональных данных Приказом по Банку назначается сотрудник Службы комплексной безопасности Банка.

6.3. Лица, ответственные за организацию обработки и защиты персональных данных, получают указания непосредственно от Председателя Правления и подотчетны ему.

6.4. Банк несет ответственность за неисполнение требований Закона «О персональных данных» в соответствии с действующим законодательством Российской Федерации.

Конкретные наказания за определенные действия/бездействие в области обработки персональных данных содержат нормы Кодекса Российской Федерации об административных правонарушениях и Уголовного кодекса Российской Федерации.

7. Сведения о реализуемых требованиях к защите персональных данных

7.1. В целях защиты персональных данных, в Банке, применяется комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (далее – СТО БР ИББС).

7.2. Банк при обработке ПДн принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. К таким мерам, в соответствии с Законом «О персональных данных» и СТО БР ИББС, в частности, относятся:

- назначение лица, ответственного за организацию обработки ПДн, и лиц, ответственных за обеспечение безопасности ПДн;

- определение угроз безопасности ПДн при их обработке;

- разработка и утверждение локальных актов по вопросам обработки и защиты ПДн;

- оценка вреда, который может быть причинен гражданам в случае нарушения Закона «О персональных данных», соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом «О персональных данных»;

- ознакомление работников Банка, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами по вопросам обработки и защиты ПДн, и обучение работников Банка;

- соблюдение условий, исключающих несанкционированный доступ к материальным носителям ПДн и к средствам защиты ПДн;

- применение технических мер защиты, включая:

- средства разграничения доступа на сетевом, прикладном и общесистемном уровнях;

- средства межсетевого экранирования;

- средства регистрации и учета действий пользователей на сетевом, прикладном и общесистемном уровнях;

- антивирусные средства защиты;

- сертифицированные средства криптографической защиты информации;

- средства обнаружения вторжений;

- средства анализа защищенности;

- средства контроля физического доступа в помещения, в которых осуществляется обработка ПДн.

- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию новой информационной системы Банка;

- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;

- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установление правил доступа к ПДн, обрабатываемым в информационных системах Банка, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн;

- осуществление внутреннего контроля и аудита соответствия обработки ПДн Закону «О персональных данных», СТО БР ИББС и подзаконным нормативным актам.

8. Справочная информация

8.1. Если после прочтения настоящего Положения у Вас остались вопросы, Вы можете получить разъяснения по всем интересующим вопросам, направив письмо на электронную почту scs@modulbank.ru, либо направить официальный запрос по почте на адрес: 156000, Костромская область, г. Кострома, улица Свердлова, д. 25а, АО КБ «Модульбанк» или на адрес: 121069, г. Москва, ул. Новодмитровская, д. 2, корп. 1, Московский Филиал АО КБ «Модульбанк».

8.2. В случае направления официального запроса в Банк, в тексте запроса необходимо указать:

- номер основного документа, удостоверяющего личность гражданина (или его законного представителя), сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие гражданина в отношениях с Банком (например, номер и дата заключения договора, условное словесное обозначение) либо сведения, иным способом подтверждающие факт обработки ПДн Банком;

- подпись гражданина (или его законного представителя). Если официальный запрос отправляется в электронном виде, то он должен быть оформлен в виде электронного документа и подписан электронной подписью в соответствии с законодательством РФ.