Утверждено
Решением Правления
АО Банк «Венец»
Протокол № 25
от 21.06.2017 г.

Положение
об обработке персональных данных в
АО Банк «Венец»

Ульяновск, 2017

Содержание

1. Общие положения

Положение об обработке персональных данных (далее — Положение) в АО Банк «Венец» (далее Банк) разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152 «О персональных данных», Федеральным законом «О банках и банковской деятельности», Федеральным законом «Об акционерных обществах», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Указом Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведения конфиденциального характера», а также документами Банка России:

- СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее - СТО БР ИББС-1.0-2014);
- СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014»

Настоящее Положение определяет цели, условия и порядок обработки персональных данных работников Банка и иных лиц, персональные данные которых подлежат обработке с использованием средств автоматизации или без использования таких средств.

Настоящее Положение устанавливает порядок предоставления, разграничения и закрытия доступа сотрудников Банка к сведениям, отнесенным к персональным данным, порядок уведомления работников Банка о факте работы с персональными данными и порядке их обработки.

Целью настоящего Положения является защита персональных данных субъектов персональных данных от несанкционированного доступа и разглашения, неправомерного их использования или утраты, 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, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, Банка России, а также утвержденными регламентами и инструкциями Банка.

Сбор, хранение, использование и распространение персональных данных лица без письменного его согласия допускаются только в случаях, предусмотренных федеральным законодательством Российской Федерации. Персональные данные относятся к категории конфиденциальной информации.

Должностные лица Банка, в обязанности которых входит ведение и использование для выполнения должностных обязанностей персональных данных субъектов персональных данных, обязаны обеспечить каждому субъекту возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

Настоящее Положение и изменения к нему утверждаются Правлением АО Банк «Венец», являются обязательным для исполнения всеми работниками Банка, имеющими доступ к персональным данным.

2. Основные понятия, термины, определения

Для целей настоящего Положения используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных - любое действие (операция) 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 (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания;

использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом Банка в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

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

уничтожение персональных данных - действия, в результате которых становится невозможным 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 становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту;

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

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.

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели

обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

информационные системы персональных данных- совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

3. Принципы обработки персональных данных

Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Банка;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

4. Способы обработки и перечень действий с персональными данными

Банк может осуществлять обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

Перечень действий с персональными данными, которые могут осуществляться Банком при обработке персональных данных субъектов:

- сбор;
- систематизация;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- обезличивание;
- блокирование;
- уничтожение;
- передача

5. Категории субъектов персональных данных

К субъектам персональных данных в Банке (далее – субъекты) относятся лица – носители персональных данных, передавшие свои персональные данные Банку (как на добровольной основе, так и в рамках выполнения требований федерального законодательства и иных нормативно-правовых актов).

Банком может осуществляться обработка персональных данных следующих категорий субъектов персональных данных:

- Физические лица, состоявшие или состоящие в договорных и иных гражданско-правовых отношениях с Банком (в т.ч. клиенты Банка);
- Физические лица, состоявшие или состоящие в трудовых отношениях с Банком, в т.ч. по совместительству (далее - работники Банка);

6. Цели обработки персональных данных

Обработка персональных данных работников Банка может осуществляться с целью организации учета работников Банка, содействия работникам в трудоустройстве, обучения, продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества; пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, иными федеральными законами.

Обработка персональных иных субъектов персональных данных, осуществляется в целях заключения (принятия решения о возможности заключения) и исполнения гражданско-правовых договоров в сфере банковской деятельности, осуществляемой на основании специального разрешения (лицензии) Банка, в т.ч :

- привлечения денежных средств юридических и физических лиц во вклады;
- размещения привлеченных во вклады денежных средств юридических и физических лиц;
- открытия и ведения банковских счетов юридических и физических лиц;
- осуществления расчетов по поручению юридических и физических лиц,

а также в целях осуществления возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, иными 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», «Об акционерных обществах», нормативными актами Банка России.

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

7. Объем и содержание персональных данных

В целях выполнения обязанностей, возложенных на Банк действующим законодательством, представителями Банка, в рамках их должностных обязанностей, обрабатываются следующие виды персональных данных: фамилия, имя, отчество (в т.ч. прежние), дата и место рождения, данные паспорта или иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ, гражданство, адрес регистрации по месту жительства (пребывания) и фактического места жительства (в случае их несовпадения), дата регистрации по месту жительства (пребывания), номера телефонов, сведения об образовании, о повышении квалификации, о трудовой деятельности, о заработной плате, о воинском учете, о номере и серии страхового свидетельства государственного пенсионного страхования, об идентификационном номере налогоплательщика, сведения из страховых полисов обязательного (добровольного) медицинского страхования, сведения о наградах, табельный номер работника АО Банк «Венец», сведения о социальных льготах и о социальном статусе.

8. Сроки обработки персональных данных

Сроки обработки указанных в п.7. Положения персональных данных определяются исходя из сроков действия договора с субъектом персональных данных, сроков хранения документов, установленных федеральными законами, нормативными документами

органов исполнительной власти Российской Федерации, в т.ч. приказом Росархива от 06.10.2000 «Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения», сроком исковой давности, а также иными требованиями законодательства и нормативными документами Банка России.

9. Порядок получения персональных данных

Все персональные данные субъекта персональных данных Банк получает непосредственно у субъектов персональных данных, за исключением случаев, предусмотренных федеральным законодательством Российской Федерации.

Банк получает сведения о персональных данных субъектов персональных данных из следующих документов и источников:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;
- документы воинского учета, содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащий сведения об образовании, профессии;
- резюме, предоставляемого соискателем работы в Банке;
- справки о заработной плате;
- анкета, заполняемая субъектом при оказании ему банковской услуги;
- иные документы и сведения, предоставляемые субъектом персональных данных при приеме на работу, прохождении производственной практики, оказании банковской услуги;
- иные документы и сведения, предоставляемые субъектом при оказании им услуг Банку (договор подряда, найма и т.д.)

Субъект персональных данных обязан представлять Банку достоверные сведения о себе. Банк имеет право проверять достоверность указанных сведений в порядке, не противоречащем действующему законодательству.

В случае предоставления персональных данных, содержащихся в документах субъекта персональных данных, сотрудник, ответственный за данный процесс, принимает от субъекта документы, в количестве и порядке, предусмотренном соответствующими внутренними нормативными документами, проверяет их полноту, правильность указываемых сведений, снимает с них копию и подшивает в соответствующее дело. Оригиналы возвращаются субъекту.

Информация, относящаяся к персональным данным работника, хранится в личном деле работника. Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа. Личные дела работников могут выдаваться на руки только Председателю Правления Банка и его заместителям и в исключительных случаях, по письменному разрешению Председателя Правления Банка, руководителю структурного подразделения.

Условием обработки персональных данных субъекта является его письменное согласие, за исключением случаев, предусмотренных федеральным законодательством Российской Федерации.

Письменное согласие субъекта на обработку его персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес оператора персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Банком способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

10. Порядок обработки персональных данных

Согласие на обработку персональных данных, которые будут обрабатываться в рамках любых договоров, в том числе трудовых договоров, договоров на оказание банковских услуг, иных договоров, также намерений заключения договоров (соискания рабочего места) должно быть получено от субъекта до начала обработки (получения) его персональных данных.

Ответственность за получение вышеуказанного согласия возлагается лично на сотрудника, ответственного за оформление данного договора или проводившего переговоры о намерении заключения договора (соискания рабочего места).

Согласия субъекта на обработку его персональных данных не требуется в следующих случаях:

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта, если получение его согласия при данных обстоятельствах невозможно;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (общедоступных персональных данных);
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами,

а также в иных, установленных федеральным законом случаях.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в письменной форме дает его законный представитель.

В случае смерти субъекта согласие на обработку его персональных данных при необходимости дает в письменной форме один из его наследников, если такое согласие не было дано субъектом персональных данных при его жизни.

В случае если Банк на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Банк не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной, частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением, если:

- субъект дал согласие в письменной форме на обработку своих соответствующих персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных;
- персональные данные относятся к состоянию здоровья субъекта и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта в данный момент невозможно;
- обработка персональных данных необходима в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации,

а также иных случаях, установленных федеральным законом.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия. При передаче персональных данных работника должностные лица Банка обязаны соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами;
- использовать персональные данные лишь в целях, для которых они сообщены. Лица, получающие персональные данные работника, обязаны соблюдать требования конфиденциальности;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации:

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Банка.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

11. Хранение персональных данных

Документы, содержащие персональные данные работника составляют его личное дело. Личное дело хранится уполномоченным лицом на бумажных носителях в сейфе; помимо этого может храниться в виде электронных документов, баз данных. Личное дело пополняется на протяжении всей трудовой деятельности работника.

Письменные доказательства получения оператором согласия субъекта персональных данных на их обработку хранятся в личном деле. Срок хранения документов работника 75 лет, если иное не определено законом.

В случаях, когда субъект, предоставивший свои персональные данные при собеседовании для получения работы в Банке, намереваясь заключить с Банком договор (как клиент и как контрагент) и т.п., не вступил в договорные отношения с Банком – письменные доказательства получения согласия оператором хранятся у уполномоченного лица в течение тридцати дней, затем уничтожаются комиссионно.

Срок хранения документов определяется законодательными актами.

При обработке персональных данных руководство Банка вправе определять способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

Юридический отдел обеспечивает правовую поддержку путем рассмотрения и согласования инструкций по обработке персональных данных.

Обеспечение техническими средствами обработки (ПЭВМ, серверами и т.д.) и их эксплуатация выполняется Управление информационных технологий

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

12. Права и обязанности субъекта персональных данных

Субъект персональных данных обязан:

- передавать Банку или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, федеральным законодательством и иными законами РФ, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др.;
- своевременно, в срок, не превышающий одного месяца, сообщать Банку об изменении своих персональных данных.

Субъект персональных данных имеет право:

- на полную информацию о своих персональных данных и об их обработке;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами. Доступ к своим персональным данным предоставляется субъекту или его законному представителю Банком при личном обращении либо при получении запроса. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Требовать от Банка исключения, исправления или 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 данных, обработанных с нарушением требований Трудового кодекса Российской Федерации и Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Указанное требование должно быть оформлено письменным заявлением субъекта персональных данных на имя Председателя Правления Банка.

Требовать об извещении Банком всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.

При отказе Банка исключить или исправить персональные данные субъекта, он имеет право заявить в письменной форме Банку о своем несогласии с соответствующим обоснованием такого несогласия. При отклонении Банком указанного обращения (несогласия), субъект персональных данных имеет право обжаловать действия Банка в порядке, предусмотренном законодательством России.

Получать информацию, касающуюся обработки его персональных данных, в том числе содержащую:

- подтверждение факта обработки персональных данных Банком, а также цель такой обработки;
- способы обработки персональных данных, применяемые Банком;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для него может повлечь за собой обработка его персональных данных.

Обжаловать в судебном порядке любые неправомерные действия или бездействия Банка при обработке и защите персональных данных.

Субъект персональных данных не должен отказываться от своих прав на сохранение и защиту охраняемой законом тайны.

Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных п. 4.1.2.10. настоящего Положения.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия субъекта в письменной форме или в случаях, предусмотренных федеральными законами.

Субъект персональных данных обладает и иными правами, закрепленными ст.14 Федерального закона «О персональных данных».

13. Права и обязанности Банка при обработке персональных данных

При сборе персональных данных Банк обязан предоставить субъекту персональных данных по его просьбе сведения, предусмотренные федеральным законом.

Если предоставление персональных данным является обязательным в соответствии с федеральным законом, Банк обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Если персональные данные получены не от субъекта персональных данных, Банк за исключением случаев, установленных законом, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- наименование и адрес Банка;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные федеральным законом права субъекта персональных данных;
- источник получения персональных данных.

Банк освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п.13 настоящего Положения, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных Банком;
- персональные данные получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- банк осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных сведений, предусмотренных 13 настоящего Положения, нарушает права и законные интересы третьих лиц.

Банк обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов.

Банк обязан рассмотреть возражение субъекта персональных данных в течение 30 рабочих дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

Если обязанность предоставления персональных данных субъектом установлена федеральным законом (включая налоговое, банковское, трудовое и иное право), Банк

обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

Банк обязан безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к нему, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Банк обязан уведомить соответствующего субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта были переданы.

Банк обязан сообщить в Уполномоченный орган по защите прав субъектов персональных данных по его законному запросу информацию, необходимую для осуществления деятельности указанного органа в установленные нормативно-правовыми актами РФ сроки.

До начала обработки персональных данных Банк обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

В банке осуществляется внутренний контроль и аудит соответствия обработки персональных данных Федеральному закону и настоящему Положению.

Настоящее Положение подлежит размещению на сайте Банка.

14. Защита персональных данных

С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в информационных системах персональных данных (далее – ИСПДн) Председателем Правления назначается служба информационной безопасности.

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам предоставляются в соответствии с их должностными инструкциями, утверждаемыми руководителем организации.

Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

Вход пользователя в систему может осуществляться по выдаваемому ему логину и электронному идентификатору согласно «Порядку предоставления доступа к информационным ресурсам АО Банк «Венец».

Каждый работник Банка, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн согласно «Инструкции по соблюдению информационной безопасности при работе с информационными ресурсами АОБанк «Венец»;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли) согласно «Положению по организации парольной защиты АО Банк «Венец»;

- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
- немедленно известить службу информационной безопасности о случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей,
- немедленно известить службу информационной о нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ;
- немедленно известить службу информационной о несанкционированных (произведенных с нарушением установленного порядка) изменениях в конфигурации программных или аппаратных средств ИСПДн;
- немедленно известить службу информационной об отклонениях в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- немедленно известить службу информационной о некорректном функционировании установленных на компьютеры технических средств защиты

Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;
- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

Служба информационной безопасности обязана:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;
- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;
- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:
- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к

элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

- вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;
- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;
- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;
- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;
- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;
- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;
- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;
- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- сопровождать подсистемы обеспечения целостности информации в ИСПДн;
- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;
- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;
- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;
- контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- поддерживать установленный порядок проведения антивирусного контроля согласно требований настоящего Положений в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

Служба информационнной безопасности имеет право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

Мероприятия, осуществляемые для организационно-технической защиты персональных данных разделяются на две части:

Мероприятия, направленные на организационные и физические аспекты защиты (описаны в настоящем положении).

Методы и способы защиты информации применяются в соответствии с классом информационных систем персональных данных. Информационные системы классифицируются, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства. Классификация информационных систем персональных данных Банка представлена в «АКТе классификации информационных систем персональных данных АО Банк «Венец».

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними («Журнал проведения инструктажа по информационной безопасности сотрудников Банка «Венец»);
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты персональных данных.

Для защиты персональных данных соблюдается ряд мер организационно-технического характера:

- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений;
- порядок доступа в помещения и перемещения сотрудников на территории Банка;

В соответствии с требованиями данного Положения при обработке защищаемой информации в ИСПДн исключается неконтролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн, определенных соответствующим приказом.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Помещения, в которых хранятся персональные данные субъектов, оборудуются надежными замками и сигнализацией на вскрытие помещений.

Для хранения персональных данных используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

Помещения, в которых хранятся персональные данные субъектов, в рабочее время при отсутствии в них работников должны быть закрыты.

Проведение уборки помещений, в которых хранятся персональные данные, должно производиться в присутствии соответствующих работников.

15. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Каждый сотрудник Банка, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность полученной информации.

Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому субъекту персональных данных, возможность ознакомления с документами и материалами, если иное не предусмотрено законом.

Неправомерный отказ в предоставлении собранных в установленном порядке персональных данных, либо несвоевременное их предоставление в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного наказания в порядке установленном Кодексом Российской Федерации об административных правонарушениях.

В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, составляющую персональные данные,

обязаны возместить причиненные убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к персональным данным.

Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения влечет наложение наказания в порядке, предусмотренном Уголовным кодексом Российской Федерации.

16. Уведомление об обработке персональных данным

Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона 152-ФЗ, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

В случае изменения сведений, указанных в части 3 статьи 22 Федерального закона №152, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Утверждено
Решением Правления
АО Банк «Венец»
Протокол № 54
от 25.07.2022 г.

Изменения и дополнения в Положение об обработке персональных данных в АО Банк «Венец»

Ульяновск, 2022

1. Изложить Раздел 5 Положения об обработке персональных данных «Категории субъектов персональных данных» в следующей редакции:

«К субъектам персональных данных в Банке (далее – субъекты) относятся лица – носители персональных данных, передавшие свои персональные данные Банку (как на добровольной основе, так и в рамках выполнения требований федерального законодательства и иных нормативно-правовых актов).

Банком может осуществляться обработка персональных данных следующих категорий субъектов персональных данных:

- Физические лица, состоявшие или состоящие в договорных и иных гражданско-правовых отношениях с Банком (в т.ч. клиенты Банка);
- Физические лица, состоявшие или состоящие в трудовых отношениях с Банком, в т.ч. по совместительству (далее - работники Банка);
- Пользователи сайта (лица, подавшие заявки на получение услуг Банка);
- Акционеры Банка, члены органов управления Банка и их близкие родственники;
- Члены семьи (близкие родственники) работников Банка»