



**Общество с ограниченной ответственностью коммерческий банк «Калуга»**

**УТВЕРЖДЕНО**  
**Протокол Правления**  
**ООО КБ «Калуга»**  
**от «15» февраля 2016 года № I-25**

## **ПОЛОЖЕНИЕ**

### **об обработке персональных данных в ООО КБ «Калуга»**

#### **1. Общие положения**

1. Положение об обработке персональных данных в ООО КБ «Калуга» (далее – «Положение») разработано в соответствии с требованиями:

- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных);
- Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 6 июля 2008 г. N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

2. Целью настоящего Положения является обеспечение требований защиты прав граждан при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

3. Персональные данные могут обрабатываться только для целей, непосредственно связанных с деятельностью ООО КБ «Калуга» (далее – «Банк»), в частности для оказания всех видов банковских услуг в соответствии с Лицензией Центрального банка Российской Федерации №1151, выданной ООО КБ «Калуга». Банк собирает данные только в объеме, необходимом для достижения названных целей.

4. Сбор, хранение, использование и распространение, в том числе передача третьим лицам, персональных данных без письменного согласия субъекта персональных данных не допускаются, за исключением случаев, предусмотренных действующим законодательством.

5. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

6. Сотрудники Банка, в обязанность которых входит обработка персональных данных субъектов персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.
7. Работники Банка, 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.
8. Настоящее Положение утверждается Протоколом Правления ООО КБ «Калуга» и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным клиентов.
9. Все сотрудники Банка, связанные с обработкой персональных данных и имеющих доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.
10. Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм настоящего Положения возлагается на назначаемого приказом по Банку сотрудника, ответственного за организацию обработки ПДн.

## **2. Основные понятия и состав персональных данных**

1. Персональные данные (далее ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).
2. Оператор – ООО КБ «Калуга» (далее - Банк).
3. 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.
4. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
5. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
6. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
7. Блокирование персональных данных - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения персональных данных).
8. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
9. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.
10. Информационная система персональных данных - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
11. Трансграничная передача персональных данных - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

## **3. Принципы обработки персональных данных**

1. Обработка ПДн должна осуществляться на законной и справедливой основе.
2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.
3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
6. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Банк должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
7. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

#### **4. Условия обработки персональных данных**

1. Обработка персональных данных допускается в следующих случаях:
  - 1.1. Обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн.
  - 1.2. Обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей.
  - 1.3. Обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем.
  - 1.4. Осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом ПДн).
  - 1.5. Осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.
2. Банк вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта. Лицо, осуществляющее обработку ПДн по поручению Банка, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом. В поручении Банка должны быть определены перечень действий с персональными данными, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки. Банком устанавливается обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн.
3. Лицо, осуществляющее обработку ПДн по поручению Банка, не обязано получать согласие субъекта ПДн на обработку его ПДн.
4. В случае, если Банк поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Банк. Лицо, осуществляющее обработку ПДн по поручению Банка, несет ответственность перед Банком.

##### **4.1. Конфиденциальность персональных данных**

Сотрудники Банка, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

##### **4.2. Общедоступные источники персональных данных**

1. В целях информационного обеспечения могут создаваться общедоступные источники ПДн. В общедоступные источники ПДн с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом ПДн.

2. Сведения о субъекте ПДн должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

### **5. Согласие субъекта персональных данных на обработку его персональных данных.**

1. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Банком.

2. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн Банк вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пунктах 1.2 – 1.5 главы 4 настоящего Положения. Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в вышеперечисленных пунктах, возлагается на Банк.

3. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя;
- наименование и адрес Банка, получающего согласие субъекта ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Банком способов обработки ПДн;
- срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта ПДн.

4. В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта ПДн.

5. В случае смерти субъекта ПДн согласие на обработку его ПДн дают наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

6. Персональные данные могут быть получены Банком от лица, не являющегося субъектом ПДн, при условии предоставления Банку подтверждения наличия оснований, указанных в пунктах 1.2 – 1.5 главы 4 настоящего Положения.

### **6. Специальные категории персональных данных**

1. Запрещается обрабатывать ПДн о политических, религиозных и философских убеждениях, а также об интимной жизни клиента Банка. Указанные специальные категории ПДн в деятельности Банка не используются и не обрабатываются.

2. Банк не вправе производить обработку данных о судимости клиента, за исключением в случаях и в порядке, которые определяются в соответствии с федеральными законами.

3. Данные о здоровье обрабатываются Банком только в том случае, если эти данные прямо относятся к возможности клиента исполнять свои обязательства перед Банком, либо используются в целях исполнения требований действующего законодательства, например, в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

Обработка указанных в настоящем пункте специальных категорий ПДн допускается в случаях, если:

- субъект ПДн дал согласие в письменной форме на обработку своих ПДн;
- персональные данные сделаны общедоступными субъектом ПДн;
- обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации;
- обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

4. Сведения о расовой и национальной принадлежности клиентов Банком не обрабатываются. Фотографии, находящиеся в документах, удостоверяющих личность клиента Банка, и иные аналогичные данные не относятся к сведениям о расовой и национальной принадлежности.

5. В случае если обработка специальных категорий ПДн клиента Банка необходима по действующему законодательству или для осуществления деятельности Банка, то такая обработка осуществляется с письменного согласия клиента, за исключением случаев, предусмотренных законодательством Российской Федерации в области ПДн.

## **7. Биометрические персональные данные**

1. Банк не обрабатывает биометрические ПДн.

2. Сканирование фотографий в документах, идентифицирующих личность клиентов (например, в паспортах), в Банке осуществляется с письменного согласия субъектов ПДн. Передаваемые в рамках договоров копии паспортов клиентов не соответствуют требованиям, предъявляемым к форматам записи изображения, установленными ГОСТ Р ИСО\ МЭК 19794-5-2006. Хранение полученных скан-копий фотографий осуществляется вместе с заключаемым с клиентом договором и в информационной системе.

## **8. Трансграничная передача персональных данных**

1. Трансграничная передача ПДн на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн, осуществляется в соответствии с Федеральным законом «О ПДн».

2. Трансграничная передача ПДн на территории иностранных государств может осуществляться в случаях:

- наличия согласия в письменной форме субъекта ПДн на трансграничную передачу его ПДн;
- исполнения договора, стороной которого является субъект ПДн;

## **9. Права субъекта персональных данных.**

1. Субъект ПДн имеет право на получение сведений, указанных в пункте 7 настоящей главы, за исключением случаев, предусмотренных пунктом 8 настоящей главы. Субъект ПДн вправе требовать от Банка уточнения его ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в пункте 7 настоящей главы, должны быть предоставлены субъекту ПДн Банком в доступной форме. В них не должны содержаться персональные данные, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

3. Сведения, указанные в пункте 7 настоящей главы, предоставляются субъекту ПДн или его представителю Банком при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Банком (номер договора, дата заключения договора, и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Банком, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. В случае, если сведения, указанные в пункте 7, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных в пункте 7 и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

5. Субъект ПДн вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных в пункте 7, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 4, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 3, должен содержать обоснование направления повторного запроса.

6. Банк вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 4 и 5 настоящей главы. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Банке.

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

- подтверждение факта обработки ПДн Банком;
- правовые основания и цели обработки ПДн;
- цели и применяемые банком способы обработки ПДн;
- наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу;

8. Право субъекта ПДн на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта ПДн к его персональным данным нарушает права и законные интересы третьих лиц;

### **9.1. Право на обжалование действий или бездействие банка**

1. Если субъект ПДн считает, что Банк осуществляет обработку его ПДн с нарушением требований Федерального закона «О Персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Банка в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.
2. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

### **10. Обязанности Банка при сборе персональных данных.**

1. Банк обязан предоставить субъекту ПДн по его просьбе информацию, предусмотренную пунктом 7 главы 9 настоящего Положения.
2. Если предоставление ПДн является обязательным в соответствии с федеральным законом, Банк обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его персональные данные.
3. Если персональные данные получены не от субъекта ПДн, Банк, за исключением случаев, изложенных в пункте 4 настоящей главы, до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:
  - адрес банка или его представителя;
  - цель обработки ПДн и ее правовое основание;
  - предполагаемые пользователи ПДн;
  - права субъекта ПДн;
  - источник получения ПДн.
4. Банк освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные пунктом 3, в случаях, если:
  - субъект ПДн уведомлен об осуществлении обработки его ПДн 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 ПДн;
  - персональные данные сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
  - предоставление субъекту ПДн сведений, предусмотренных пунктом 3, нарушает права и законные интересы третьих лиц;
  - При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", Банк обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на серверах банка, расположенных на территории Российской Федерации по адресу: г. Калуга, ул. Суворова, д. 147, в помещении ограниченного доступа.

#### **10.1. Меры, направленные на обеспечение выполнения обязанностей Банком.**

1. Банк обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О Персональных данных» и принятым в соответствии с ним Положением о ПДн. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения своих обязанностей. К таким относятся:
  - назначение ответственного за организацию обработки ПДн;
  - издание документов, определяющих политику банка в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение, выявление нарушений и устранение последствий таких нарушений;
  - применение организационных и технических мер по обеспечению безопасности ПДн в соответствии с главой 10.4 настоящего Положения;
  - осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону «О персональных данных» и настоящему Положению, требованиям к защите ПДн, политике Банка в отношении обработки ПДн;

▪ оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения своих обязанностей;

▪ ознакомление работников Банка, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Банка в отношении обработки ПДн, проведение инструктажа указанных работников.

2. Банк обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн. В случае осуществления Банком сбора ПДн с использованием информационно-телекоммуникационных сетей, Банк обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Банк обязан представить документы, указанные в подпункте 1 пункта 10.1 главы 10, и (или) иным образом подтвердить принятие мер по запросу уполномоченного органа по защите прав субъектов ПДн.

### **10.2. Обязанности Банка при обращении субъекта ПДн либо при получении запроса субъекта ПДн или его представителя, а также уполномоченного органа по защите прав субъектов ПДн**

1. Банк обязан сообщить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта ПДн или его представителя в течение тридцати дней с момента даты получения запроса субъекта ПДн или его представителя.

2. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя Банк обязан дать в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя с момента даты получения запроса субъекта ПДн или его представителя.

3. Банк обязан предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту ПДн. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Банк обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Банк обязан уничтожить такие персональные данные и уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах. Принять меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Банк обязан сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с момента даты получения такого запроса.

### **10.3. Обязанности Банка по устранению нарушений законодательства, допущенных при обработке ПДн, по уточнению, блокированию и уничтожению ПДн.**

1. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки. В случае



выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

2. В случае подтверждения факта неточности ПДн Банк на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

3. В случае выявления неправомерной обработки ПДн, осуществляемой Банком или лицом, действующим по поручению Банка, в срок, не превышающий трех рабочих дней с момента даты этого выявления, Банк обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по его поручению. В случае, если обеспечить правомерность обработки ПДн невозможно, Банк в срок, не превышающий десяти рабочих дней с момента даты выявления неправомерной обработки ПДн, обязан уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении ПДн Банк уведомляет субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя, либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом, указанный орган.

4. В случае достижения цели обработки ПДн Банк прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и уничтожает персональные данные в срок, не превышающий тридцати дней с момента даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн.

5. В случае отзыва субъектом ПДн согласия на обработку его ПДн Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется лицом, действующим по поручению Банка) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить персональные данные в срок, не превышающий тридцати дней с момента даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн, а также предусмотренных другими федеральными законами.

6. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в пунктах 3-5 настоящего Положения, Банк осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется лицом, действующим по поручению Банка) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

#### **10.4. Меры по обеспечению безопасности персональных данных при их обработке**

1. Банк при обработке персональных данных принимает необходимые правовые, организационные и технические меры и обеспечивает 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.

2. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных и составлением модели угроз;
- определением уровня защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

- проведением мероприятий по защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленный уровень защищенности персональных данных;
- 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;
- применением прошедших в установленном порядке процедуру оценки соответствия применяемых мер защиты информации;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 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;
- контролем над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Использование и хранение биометрических ПДн (в случае их наличия) вне информационных систем ПДн осуществляются только на материальных носителях информации с применением технологии ее хранения, которая обеспечивает защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

4. Меры по защите персональных данных, обрабатываемых на автоматизированных системах и в автоматизированных рабочих местах, определяются и реализуются Банком в соответствии с требованиями стандарта Банка России СТО БР ИББС-1.0, а также «Политикой информационной безопасности в ООО КБ «Калуга».

## **11. Уведомление об обработке персональных данных.**

1. Банк до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных пунктом 2 данной главы.

2. Банк вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

- обрабатываемых в соответствии с трудовым законодательством;
- полученных Банком в связи с заключением договора, стороной которого является субъект ПДн, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются Банком исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;
- сделанных субъектом ПДн общедоступными;
- включающих в себя только фамилии, имена и отчества субъектов ПДн;
- необходимых в целях однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях;
- включенных в информационные системы ПДн, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности ПДн при их обработке и к соблюдению прав субъектов ПДн;

3. Уведомление, предусмотренное частью 1 настоящей Главы, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

- наименование, адрес Банка;
  - 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 пунктом 10.1 главы 10 и главой 11 настоящего Положения, 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 ПДн, 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 о месте нахождения базы данных информации, содержащие ПДн граждан РФ;
  - сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.
4. В случае изменения сведений, указанных в пункте 3 настоящей главы, а также в случае прекращения обработки ПДн Банк обязан уведомить об этом уполномоченный орган по защите прав субъектов ПДн в течение десяти рабочих дней с момента даты возникновения таких изменений или с момента даты прекращения обработки персональных данных.

## **12. Ответственность за организацию обработки персональных данных.**

- 1 Банк назначает лицо, ответственное за организацию обработки персональных данных, которое получает указания непосредственно от Председателя Правления Банка и подотчетно ему.
2. Сотрудники банка обязаны предоставлять лицу, ответственному за организацию обработки ПДн, сведения, указанные в пункте 3 главы 11 настоящего Положения.
3. Лицо, ответственное за организацию обработки ПДн, в частности, обязано:
- осуществлять внутренний контроль над соблюдением работниками Банка Закона РФ «О персональных данных», в том числе требований к защите персональных данных;
  - доводить до сведения работников положения законодательства Российской Федерации о персональных данных, настоящего Положения, требований к защите персональных данных;
  - организовать работу по приему и обработке обращений и запросов субъектов ПДн или их представителей и осуществлять контроль за обработкой таких обращений и запросов.
4. Банк ответственен за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность сотрудников за соблюдением установленных в Банке принципов уважения приватности.
5. Все лица, связанные с получением, обработкой и защитой ПДн субъекта обязаны подписать «Обязательство о неразглашении персональных данных Субъекта персональных данных» (приложение 1).
6. Банк обязуется поддерживать систему приема, регистрации и контроля рассмотрения жалоб Субъектов персональных данных, доступную как посредством использования Интернета, так и с помощью телефонной, телеграфной или почтовой связи.
7. Лица, виновные в нарушении требований настоящего Положения привлекаются к дисциплинарной ответственности.

**Заместитель начальника отдела безопасности**

**А.А. Наумов**



**общество с ограниченной ответственностью коммерческий банк «Калуга»  
(ООО КБ «Калуга»)**

**ОБЯЗАТЕЛЬСТВО**  
**о неразглашении персональных данных Субъекта персональных данных**

г.Калуга

«\_\_» \_\_\_\_\_ 20\_\_ года

Я, \_\_\_\_\_, понимаю, что получаю доступ к персональным данным Субъекта ПДн. Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой и хранением персональных данных Субъектов ПДн.

Я понимаю, что разглашение такого рода информации может нанести ущерб Субъектам ПДн как прямой, так и косвенный.

В связи с этим даю обязательство при обработке (сборе, хранением, передаче, уточнении) персональных данных Субъекта персональных данных соблюдать все описанные в «Положении об обработке персональных данных в ООО КБ «Калуга»» требования.

Я предупрежден(-а) о том, что в случае разглашения мной сведений, касающихся персональных данных Субъекта персональных данных или их утраты, я несу ответственность в соответствии с действующим законодательством Российской Федерации.

С «Положением об обработке персональных данных в ООО КБ «Калуга»» ознакомлен(-а).

\_\_\_\_\_  
Личная подпись

\_\_\_\_\_  
Фамилия И.О.