

**ПОЛОЖЕНИЕ**  
**по обработке и защите персональных данных**  
**в АКБ «Алмазэргиэнбанк» АО**

город Якутск  
2016 год

## 1. Общие положения

1.1. Настоящее Положение по обработке и защите персональных данных (далее — Положение) АКБ «Алмазэргиэнбанк» АО (далее – Банк) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Трудовым кодексом РФ, иными нормативными правовыми актами, действующими на территории Российской Федерации.

1.2. Цель разработки Положения — определение порядка обработки персональных данных в Банке; обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения Председателем Правления и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом.

1.4. Все работники Банка должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных в отношении персональных данных работников Банка снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Банка, если иное не определено законом.

1.6. Контроль за соблюдением настоящего Положения осуществляет администратор информационной безопасности (ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных) и ответственный за организацию обработки персональных данных, назначаемые в соответствии с приказом Председателя Правления.

1.7. Персональные данные являются конфиденциальной информацией, охраняемой в соответствии с действующим законодательством Российской Федерации, и на них распространяются все требования, установленные внутренними документами Банка, связанными с обеспечением защиты конфиденциальной информации.

## 2. Основные понятия и состав персональных данных

2. Для целей настоящего Положения используются следующие основные понятия и определения:

- **«персональные данные»** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- **«оператор»** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;
- **«субъект»** - субъект персональных данных;
- **«обработка персональных данных»** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение

(обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- **«распространение персональных данных»** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- **«использование персональных данных»** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- **«блокирование персональных данных»** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- **«уничтожение персональных данных»** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- **«обезличивание персональных данных»** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
- **«информационная система персональных данных»** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- **«конфиденциальность персональных данных»** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
- **«трансграничная передача персональных данных»** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;
- **«общедоступные персональные данные»** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
- **«информация»** - сведения (сообщения, данные) независимо от формы их представления.
- **«доступ к информации»** - возможность получения информации и ее использования;
- **«документированная информация»** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

### **3. Цели и задачи обработки персональных данных**

3.1. В соответствии с разделом 2 настоящего Положения оператором, организующим и осуществляющим обработку персональных данных, является АКБ «Алмазэргиэнбанк» АО.

3.2. К персональным данным относятся:

3.2.1 Сведения, содержащиеся в основном документе, удостоверяющем личность субъекта.

3.2.2. Сведения о месте жительства субъекта.

3.2.3. Информация, содержащаяся в трудовой книжке работника.

3.2.4. Сведения об образовании, квалификации или наличии специальной подготовки.

3.2.5. Сведения о заработной плате работников.

3.2.6. Иные сведения.

3.3. Обработка персональных данных в Банке осуществляется:

как без использования средств автоматизации, так и с использованием автоматизированных информационных систем: 1С:Предприятие – Зарплата и управление Персоналом КОРП, ПК «Зарплата-КС», Система «СБиС++: Электронная отчетность», E-staff Рекрутер, Пакет офисных приложений Microsoft Office.

3.4. При принятии решений, затрагивающего интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

#### **4. Субъекты персональных данных**

4.1. В соответствии с разделом 2 настоящего Положения к субъектам персональных данных относятся следующие категории физических лиц:

- работники Банка;
- контрагенты;

4.2. Все персональные данные субъекта персональных данных оператору следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Банка должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

4.3. Банк не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

4.4. Субъект персональных данных самостоятельно принимает решение о предоставлении своих персональных данных и дает согласие на их обработку.

Обработка указанных персональных данных возможна только с их согласия, либо без их согласия в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

4.5. Субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны.

4.6. Согласие на обработку персональных данных оформляется в письменном виде.

Письменное согласие на обработку своих 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 (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

4.7. В случаях, когда оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении оператор обязан сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах: один из которых предоставляется субъекту, второй хранится у оператора.

4.8. В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные данные следует получать от его законных представителей.

4.9. Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.

4.10. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному запросу на имя руководителя организации.

4.11. Субъект персональных данных имеет право на получение следующей информации: - 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 субъекта персональных данных может повлечь за собой обработка его персональных данных.

4.12. Субъект персональных данных вправе требовать от оператора 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.

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

4.14. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при получении письменного запроса субъекта персональных данных или его законного представителя. Письменный запрос должен быть адресован на имя Председателя Правления или уполномоченного Председателем лицо.

4.15. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Оператора при обработке и защите его персональных данных.

## **5. Состав персональных данных, обрабатываемых с использованием автоматизированных информационных систем**

5.1. Состав персональных данных, обрабатываемых с использованием автоматизированных информационных систем Банка, определяется настоящим Положением и соответствует целям и задачам сбора, обработки и использования персональных данных в соответствии с разделом 3 настоящего Положения.

5.2. Перечень персональных данных автоматизированных информационных систем Банка зависит от категории субъекта персональных данных и утверждается Председателем Правления Банка.

## **6. Порядок сбора, хранения и использования персональных данных**

6.1. Субъекты персональных данных при получении от них согласия на обработку персональных данных в автоматизированных информационных системах должны быть ознакомлены с перечнем собираемых и используемых сведений, с целями и задачами сбора, хранения и использования персональных данных.

6.2. Персональные данные субъектов персональных данных могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

6.3. Порядок хранения анкет и иных документов, содержащих информацию персонального характера, а также согласий на обработку персональных данных определяются внутренними документами Банка.

6.4. Ввод персональных данных в автоматизированные информационные системы Банка осуществляется работником, имеющим доступ к работе с персональными данными, и в соответствии с его должностными обязанностями. На бумажном носителе информации, содержащей персональные данные (анкеты, личные листки и др.) работник,

осуществляющий ввод данных, оставляет отметку о дате ввода информации и о лице, осуществившем ее ввод.

6.5. Сотрудники, осуществляющие ввод и обработку данных с использованием автоматизированных информационных систем, несут ответственность за достоверность и полноту введенной информации.

6.6. При работе с программными средствами автоматизированных информационных систем Банка, реализующими функции просмотра и редактирования персональных данных, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующих должностных обязанностей.

6.7. Хранение персональных данных в автоматизированных информационных системах Банка осуществляется на серверах Банка с использованием специализированного программного обеспечения, отвечающего требованиям безопасности.

6.8. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по истечению установленных сроков хранения информации, по достижении целей обработки или в случае утраты необходимости в их достижении.

6.9. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

6.10. Хранение резервных и технологических копий баз данных автоматизированных информационных систем, содержащих информацию персонального характера, осуществляется на серверах организации и сменных носителях, доступ к которым ограничен.

6.11. Вынос резервных и технологических копий баз данных автоматизированных информационных систем, содержащих информацию персонального характера, из организации запрещен. Передача и копирование резервных и технологических копий баз данных допустима только для прямого использования с целью технологической поддержки автоматизированных информационных систем.

6.12. Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения руководителя или уполномоченного им лица.

## **7. Особенности предоставления доступа к персональным данным**

7.1. Доступ сотрудников к персональным данным, содержащимся как в автоматизированных информационных системах организации, так и на бумажных носителях осуществляется с письменного согласия руководителя организации или уполномоченного им лица (допуск).

7.2. Сотрудник, получивший допуск к персональным данным, должен быть ознакомлен с настоящим Положением.

7.3. При получении доступа к персональным данным сотрудники подписывают обязательство о неразглашении персональных данных.

7.4. Доступ к автоматизированным информационным системам Банка ограничен политикой безопасности системы, реализуемой с использованием технических и организационных мероприятий.

7.5. Каждый пользователь имеет индивидуальную учетную запись, которая определяет его права и полномочия в автоматизированных информационных системах. Информация об учетной записи не может быть передана другим лицам. Пользователь несет персональную ответственность за конфиденциальность сведений собственной учетной записи.

Запрещается использование для доступа к автоматизированным информационным системам Организации учетных записей других пользователей.

7.6. Созданием, удалением и изменением учетных записей пользователей автоматизированных информационных систем занимаются сотрудники Службы ИБ в соответствии с должностными обязанностями.

7.7. При получении доступа к персональным данным сотрудники подписывают обязательство о неразглашении персональных данных.

7.8. Право доступа к персональным данным субъектов персональных данных имеют:

- Председатель Правления Банка;
- Заместители Председателя Правления;
- главный бухгалтер;
- сотрудники Банка, в части их касающейся.

## **8. Порядок передачи информации, содержащей персональные данные**

8.1. В соответствии с законодательством Российской Федерации персональные данные работников Банка, либо клиентов Банка могут быть переданы правоохранительным, судебным органам и другим учреждениям в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства, а также в случаях, установленных федеральным законом.

8.2. Запрещается сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия. Обработка персональных данных субъектов персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

8.3. Передача информации третьей стороне возможна только при письменном согласии работников.

## **9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

9.1. Нарушение требований настоящего Положения может повлечь гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

9.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.