

«УТВЕРЖДЕНО»

Протоколом правления АО «ALFA INVEST
sug'urta kompaniyasi» от 06.08 2026 года



Председатель правления
Ахметова И.Ю.

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ
АО «ALFA INVEST sug'urta kompaniyasi»

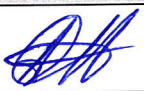
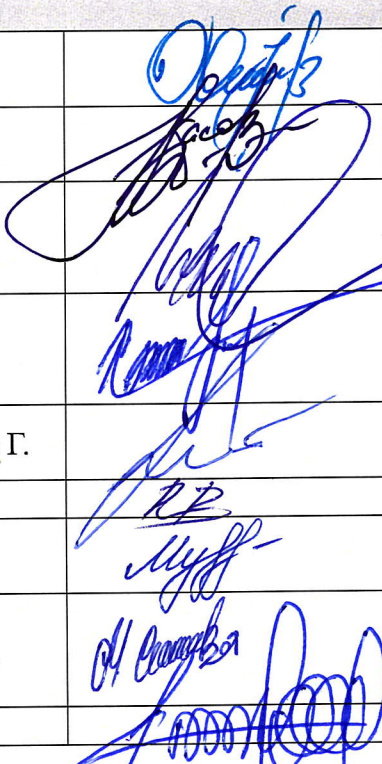
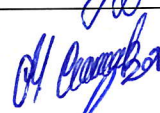
Ташкент 2026 г.

1. КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА

1.1 РАЗРАБОТАН И ВНЕСЕН

1.2 ВВЕДЕН В ДЕЙСТВИЕ «06» августа 2026 г.

Регистрационный код ТПТ/ИДА-01.

Должность	ФИО	Подпись	Дата
РАЗРАБОТАНО			
Юрист корпоративного права	Абдуманонов А.		
СОГЛАСОВАНО			
Заместитель председателя по страхованию	Хусанов А.		
Заместитель председателя по финансам	Аббасов Б.		
Заместитель председателя по андеррайтингу и перестрахованию	Гареева Р.		
Врио Заместителя председателя по юридическим вопросам	Хусанов М.		
Начальник Службы безопасности	Нурмухамедов Г.		
Директор Департамента ИТ	Садиков С.		
Начальник Службы регуляторной отчетности	Мустафин Л.		
Директор Департамента урегулирования страховых претензий	Санакулова М.		
Главный бухгалтер	Тухтаев Ш.		

2. Общие положения

2.1. Настоящая Политика конфиденциальности и защиты персональных данных АО «ALFA INVEST sug'urta kompaniyasi» определяет общие принципы, организационные меры, порядок внутреннего контроля, распределение ответственности между структурными подразделениями, а также правила обработки и защиты персональных данных в АО «ALFA INVEST sug'urta kompaniyasi» (далее по тексту – «Компания»).

2.2. Настоящая Политика разработана в соответствии с Законом Республики Узбекистан «О персональных данных» от 02 июля 2019 года № ЗРУ-547, законодательством о страховой деятельности, законодательством о бухгалтерском учете, налоговом учете, электронном документообороте, архивном деле, обращениях физических и юридических лиц, а также внутренними документами Компании.

2.3. Настоящая Политика применяется ко всем персональным данным, полученным Компанией:

- через цифровые сервисы Компании;
- при личном обращении физических лиц в офисы Компании;
- путем подачи заявлений, анкет, договоров, актов, доверенностей, претензий, жалоб и иных документов на бумажном носителе;
- посредством электронной почты;

- посредством контакт-центра;
- посредством почтовой связи;
- через страховых агентов, партнеров и посредников;
- от банков, платежных организаций и иных финансовых организаций;
- от сервисных, ремонтных, медицинских, экспертных, оценочных и иных организаций;
- от государственных органов, судов, правоохранительных органов и иных уполномоченных лиц;
- из информационных систем, баз данных, реестров и иных источников в случаях, допускаемых законодательством.

2.4. Настоящая Политика распространяется на обработку персональных данных как в электронной форме, так и на бумажных и иных материальных носителях.

2.5. Настоящая Политика является общедоступным документом и размещается в цифровых сервисах Компании, а также может быть предоставлена субъекту персональных данных по его запросу.

2.6. Компания организует обработку персональных данных таким образом, чтобы обеспечить законность, прозрачность, безопасность, минимизацию обрабатываемых данных и ограничение доступа к ним только тем лицам, которым такие данные необходимы для выполнения служебных обязанностей.

3. Принципы обработки персональных данных

3.1. Компания при обработке персональных данных руководствуется следующими принципами:

- законность обработки;
- обработка персональных данных только для конкретных, заранее определенных и законных целей;
- недопущение обработки избыточных персональных данных;
- соответствие объема персональных данных целям обработки;
- достоверность, точность и актуальность персональных данных;
- ограничение срока хранения персональных данных;
- обеспечение конфиденциальности и безопасности персональных данных;
- разграничение доступа работников к персональным данным;
- использование персональных данных только в рамках служебной необходимости;
- недопущение передачи персональных данных третьим лицам без правового основания;
- обеспечение прав субъектов персональных данных;
- внутренний контроль соблюдения требований настоящей Политики.

3.2. Компания не должна запрашивать и обрабатывать персональные данные, которые не связаны с конкретной целью обработки, страховым продуктом, договором страхования, заявлением, страховым случаем, выплатой, обращением или требованием законодательства.

4. Правовые основания обработки персональных данных

4.1. Компания обрабатывает персональные данные при наличии одного или нескольких следующих оснований:

- согласие субъекта персональных данных;
- необходимость заключения и исполнения договора страхования;
- необходимость рассмотрения заявления, обращения, претензии или требования субъекта персональных данных;
- исполнение требований законодательства Республики Узбекистан;
- исполнение обязанностей по бухгалтерскому, налоговому, страховому, архивному и иному обязательному учету;
- необходимость защиты прав и законных интересов Компании, субъекта персональных данных или третьих лиц;

- иные основания, предусмотренные законодательством Республики Узбекистан.

4.2. В случаях, когда обработка персональных данных осуществляется на основании согласия, Компания обеспечивает возможность получения, фиксации и хранения такого согласия в бумажной или электронной форме.

4.3. Отзыв согласия не влияет на законность обработки персональных данных, осуществленной до момента получения такого отзыва, а также не препятствует дальнейшей обработке данных в случаях, когда такая обработка требуется по законодательству, договору страхования, правилам бухгалтерского, налогового, страхового или архивного учета либо необходима для защиты прав и законных интересов Компании.

5. Источники получения персональных данных

5.1. Компания может получать персональные данные:

- непосредственно от субъекта персональных данных;
- через цифровые сервисы Компании;
- из документов, загруженных или предоставленных субъектом персональных данных;
- из заявлений, обращений, претензий и жалоб;
- из личного кабинета;
- от представителей субъекта персональных данных;
- от страховых агентов и партнеров;
- от банков, платежных организаций и иных финансовых организаций;
- от сервисных, ремонтных, медицинских, экспертных и оценочных организаций;
- от ассистанс-компаний;
- от перестраховщиков и состраховщиков;
- от государственных органов, судов, правоохранительных органов, нотариусов и иных уполномоченных лиц;
- из информационных систем, баз данных, реестров и иных источников в случаях, допускаемых законодательством.

5.2. Если персональные данные предоставляются не самим субъектом персональных данных, лицо, предоставившее такие данные, должно иметь согласие субъекта персональных данных или иное законное основание для их предоставления Компании.

6. Распределение ответственности между структурными подразделениями

6.1. Ответственность за соблюдение требований настоящей Политики распределяется между структурными подразделениями Компании в зависимости от их функций, доступа к персональным данным и участия в процессах обработки.

6.2. Структурное подразделение, осуществляющее продажу страховых продуктов:

- осуществляют сбор персональных данных, необходимых для консультирования клиентов, оформления страховых продуктов, заключения и сопровождения договоров страхования;
- обеспечивают получение необходимых согласий субъектов персональных данных;
- проверяют полноту и корректность данных, предоставленных страхователем, застрахованным лицом, выгодоприобретателем или представителем;
- не запрашивают избыточные персональные данные, не связанные с конкретным страховым продуктом или обращением;
- передают документы и данные в другие подразделения Компании только в пределах служебной необходимости;
- обеспечивают конфиденциальность сведений, полученных при взаимодействии с клиентами;
- незамедлительно информируют ответственное подразделение о выявленных ошибках, неточностях или нарушениях при обработке персональных данных.

6.3. Структурное подразделение, осуществляющее урегулирование убытков:

- обрабатывает персональные данные, необходимые для рассмотрения заявлений о страховом случае;
- осуществляет сбор и анализ документов, подтверждающих обстоятельства страхового случая, размер ущерба и право на получение страхового возмещения;
- взаимодействует с экспертами, оценщиками, медицинскими организациями, автосервисами, ассистанс-компаниями, аварийными комиссарами и иными лицами, участвующими в урегулировании страхового случая;
- обеспечивает соблюдение конфиденциальности страховой, медицинской и иной охраняемой законом информации;
- передает персональные данные третьим лицам только в объеме, необходимом для урегулирования страхового случая;
- обеспечивает хранение материалов страхового случая в порядке и сроки, установленные законодательством и внутренними документами Компании.

6.4. Структурное подразделение, осуществляющее андеррайтинг:

- обрабатывает персональные данные в целях оценки страхового риска, определения условий страхования и расчета страховой премии;
- анализирует сведения об объекте страхования, страховых рисках, предыдущих убытках, состоянии здоровья, имущественном положении и иных обстоятельствах, если такие сведения необходимы для конкретного вида страхования;
- обеспечивает принятие решений по страхованию на основании достаточных и относимых данных;
- не допускает использования персональных данных в целях, не связанных с оценкой страхового риска и заключением договора страхования;
- обеспечивает ограничение доступа к андеррайтинговым материалам.

6.5. Структурное подразделение, осуществляющее бухгалтерский учет и отчетность, статистику и анализ данных, а также финансовое подразделение:

- обрабатывают персональные данные в целях приема и учета страховых премий, осуществления страховых выплат, возврата части страховой премии, ведения бухгалтерского, налогового, финансового, управленческого, статистического и аналитического учета;
- обеспечивают корректное отражение операций, связанных с персональными данными, в учетных, финансовых, управленческих, статистических и аналитических системах Компании;
- осуществляют подготовку внутренней управленческой, финансовой, страховой, статистической, аналитической и иной отчетности Компании;
- используют персональные данные для анализа страхового портфеля, страховых премий, страховых выплат, убыточности, динамики продаж, клиентских обращений, качества обслуживания, эффективности страховых продуктов и иных показателей деятельности Компании;
- по возможности используют обезличенные и/или агрегированные данные при подготовке аналитических, статистических и управленческих материалов;
- не допускают использования персональных данных в целях, не связанных с бухгалтерским, налоговым, финансовым, страховым, статистическим, аналитическим и управленческим учетом;
- хранят платежные, финансовые, учетные, статистические и аналитические документы в сроки, установленные законодательством и внутренними документами Компании;
- передают персональные данные банкам, платежным организациям, государственным органам и иным уполномоченным лицам только в случаях и пределах, необходимых для исполнения финансовых, налоговых, отчетных и иных обязательств Компании;
- обеспечивают конфиденциальность банковских реквизитов, платежных документов, сведений о финансовом положении субъектов персональных данных, а также иной информации, обрабатываемой в рамках бухгалтерского, финансового, статистического и аналитического учета.

6.6. Юридический департамент:

- обеспечивает правовое сопровождение вопросов обработки персональных данных;
- участвует в разработке, актуализации и правовой экспертизе внутренних документов Компании по вопросам персональных данных;
- рассматривает обращения субъектов персональных данных, связанные с реализацией их прав, отзывом согласия, требованием об уточнении, прекращении обработки или уничтожении данных;
- участвует в оценке правомерности передачи персональных данных третьим лицам;
- обеспечивает защиту прав и законных интересов Компании в претензионном, судебном, регрессном и суброгационном порядке;
- участвует в расследовании инцидентов, связанных с неправомерной обработкой или раскрытием персональных данных.

6.7. Служба безопасности

- осуществляет мероприятия по защите персональных данных от неправомерного доступа, раскрытия, изменения, копирования, уничтожения или иного неправомерного использования;
- участвует в расследовании инцидентов, связанных с нарушением конфиденциальности или безопасности персональных данных;
- контролирует соблюдение режима доступа к персональным данным в пределах своей компетенции;
- участвует в проверке работников, подрядчиков и иных лиц, имеющих доступ к персональным данным, в случаях и порядке, допускаемых законодательством.

6.8. Департамент IT:

- обеспечивает техническую защиту информационных систем, в которых обрабатываются персональные данные;
 - организует разграничение прав доступа, аутентификацию, ведение журналов доступа, резервное копирование и восстановление данных;
 - принимает меры по предотвращению несанкционированного доступа, утечки, утраты, изменения или уничтожения персональных данных;
 - обеспечивает безопасность цифровых сервисов, личного кабинета, платежных страниц, CRM-систем, систем урегулирования убытков, бухгалтерских систем и иных информационных систем Компании;
 - взаимодействует с IT-подрядчиками, хостинг-провайдерами, операторами информационных систем и техническими поставщиками в пределах заключенных договоров;
 - незамедлительно информирует юридическое подразделение и службу безопасности о технических инцидентах, которые могут повлечь нарушение безопасности персональных данных.
- обеспечивает хранение персональных данных, подлежащих обязательному хранению на территории Республики Узбекистан, в информационных системах, базах данных, серверах, облачных или иных технических решениях, размещенных на территории Республики Узбекистан;
- не допускает размещение, хранение или обработку за пределами Республики Узбекистан персональных данных, в отношении которых законодательством установлено требование обязательного хранения на территории Республики Узбекистан, за исключением случаев, прямо допускаемых законодательством;
- обеспечивает техническую возможность учета, идентификации и разграничения баз персональных данных, подлежащих обязательному хранению на территории Республики Узбекистан;
- обеспечивает ведение и сохранность технических журналов доступа к информационным системам, в которых обрабатываются персональные данные;
- обеспечивает резервное копирование персональных данных с соблюдением требований законодательства о персональных данных, информационной безопасности и локализации данных;
- при привлечении IT-подрядчиков, хостинг-провайдеров, облачных сервисов, операторов информационных систем и иных технических поставщиков предварительно проверяет возможность соблюдения ими требований законодательства Республики Узбекистан о

персональных данных, включая требования к хранению данных на территории Республики Узбекистан;

не допускает подключение внешних сервисов, модулей, API, аналитических инструментов, облачных решений и иных технических средств, если их использование может привести к незаконной передаче, хранению или обработке персональных данных за пределами Республики Узбекистан;

совместно с юридическим подразделением и службой безопасности участвует в проверке договоров с IT-подрядчиками на предмет наличия обязательств по конфиденциальности, защите персональных данных, запрету их использования в самостоятельных целях и соблюдению требований законодательства Республики Узбекистан;

обеспечивает техническое исполнение требований субъекта персональных данных о временном приостановлении обработки, ограничении доступа, изменении, дополнении, уничтожении или обезличивании персональных данных, если такое требование подлежит исполнению в соответствии с законодательством.

6.9. Инспектор кадрового производства:

- обеспечивает ознакомление работников Компании с требованиями настоящей Политики и иных внутренних документов по вопросам обработки персональных данных;
- организует заключение соглашения о неразглашении конфиденциальной информации и персональных данных;
- участвует в обучении работников правилам обработки и защиты персональных данных;
- ведет учет работников, имеющих доступ к персональным данным в связи с исполнением трудовых обязанностей;
- взаимодействует с руководителями структурных подразделений по вопросам изменения, предоставления или прекращения доступа работников к персональным данным.

6.10. Руководители структурных подразделений:

- несут ответственность за соблюдение требований настоящей Политики в подчиненных подразделениях;
- обеспечивают доступ работников к персональным данным только в пределах их должностных обязанностей;
- контролируют недопущение избыточного сбора, копирования, хранения и передачи персональных данных;
- обеспечивают своевременное прекращение доступа работников к персональным данным при изменении должностных обязанностей, переводе или прекращении трудового договора;
- незамедлительно информируют юридическое подразделение, службу безопасности и IT-подразделение о выявленных нарушениях или инцидентах, связанных с персональными данными.

6.11. Работники Компании:

- обязаны обрабатывать персональные данные только в пределах своих должностных обязанностей;
- не вправе передавать персональные данные третьим лицам без законного основания и соответствующего разрешения;
- обязаны соблюдать конфиденциальность персональных данных, страховой тайны, врачебной тайны и иной охраняемой законом информации;
- обязаны использовать персональные данные только в целях, для которых они были получены;
- обязаны незамедлительно сообщать руководителю подразделения, юридическому подразделению, службе безопасности или IT-подразделению о фактах утраты, раскрытия, неправомерного доступа или иного нарушения безопасности персональных данных;
- несут ответственность за нарушение требований законодательства, настоящей Политики и внутренних документов Компании.

7. Передача персональных данных третьим лицам

7.1. Компания может передавать персональные данные третьим лицам только в случаях, когда такая передача необходима для достижения целей обработки, исполнения договора страхования, урегулирования страхового случая, осуществления страховой выплаты, исполнения требований законодательства или защиты прав и законных интересов Компании.

7.2. Передача персональных данных третьим лицам осуществляется только в объеме, необходимом для достижения соответствующей цели.

7.3. Компания не передает персональные данные третьим лицам для самостоятельного маркетингового использования таких лиц без отдельного согласия субъекта персональных данных.

7.4. В договорах с третьими лицами, которым передаются персональные данные или поручается их обработка, должны предусматриваться обязательства по соблюдению конфиденциальности, обеспечению безопасности персональных данных и запрету использования данных в целях, не связанных с поручением Компании.

7.5. Трансграничная передача персональных данных осуществляется в пределах целей обработки персональных данных и при соблюдении требований законодательства Республики Узбекистан.

7.6. При трансграничной передаче персональных данных Компания принимает разумные меры для обеспечения конфиденциальности и безопасности передаваемых данных.

8. Хранение персональных данных на территории Республики Узбекистан и регистрация баз персональных данных

8.1. Компания обеспечивает хранение и обработку персональных данных с соблюдением требований законодательства Республики Узбекистан, включая требования к хранению отдельных категорий персональных данных на территории Республики Узбекистан.

8.2. Персональные данные, в отношении которых законодательством установлено требование обязательного хранения на территории Республики Узбекистан, подлежат хранению в информационных системах, базах данных, серверах, облачных или иных технических решениях, размещенных на территории Республики Узбекистан.

8.3. К персональным данным, подлежащим обязательному хранению на территории Республики Узбекистан, относятся, в том числе, биометрические и генетические данные физических лиц, если такие данные обрабатываются Компанией.

8.4. Трансграничная передача, хранение или обработка персональных данных за пределами Республики Узбекистан допускается только в случаях и порядке, предусмотренных законодательством Республики Узбекистан, договором, согласием субъекта персональных данных либо при наличии иного законного основания.

8.5. Компания обеспечивает регистрацию баз персональных данных в Государственном реестре баз персональных данных в случаях, когда такая регистрация является обязательной в соответствии с законодательством Республики Узбекистан.

8.6. Ответственными за контроль соблюдения требований по хранению персональных данных на территории Республики Узбекистан являются IT-подразделение, юридическое подразделение и служба безопасности в пределах их компетенции.

8.7. До внедрения новой информационной системы, цифрового сервиса, CRM-системы, платежного модуля, облачного решения, API-интеграции или иного технического инструмента, связанного с обработкой персональных данных, IT-подразделение совместно с юридическим подразделением и службой безопасности оценивает соответствие такого решения требованиям законодательства о персональных данных.

9. Сроки хранения персональных данных

9.1. Персональные данные хранятся не дольше, чем это необходимо для достижения целей обработки, если более длительный срок хранения не предусмотрен законодательством, договором

страхования, правилами страхования, требованиями бухгалтерского, налогового, страхового или архивного учета.

9.2. Персональные данные, связанные с договорами страхования, страховыми выплатами, бухгалтерским учетом, налоговым учетом, судебными спорами, претензионной работой, регрессом и суброгацией, могут храниться в течение сроков, установленных законодательством Республики Узбекистан и внутренними документами Компании.

9.3. После достижения целей обработки или истечения срока хранения персональные данные подлежат уничтожению, обезличиванию или блокированию, если иное не предусмотрено законодательством.

9.4. Уничтожение персональных данных осуществляется таким образом, чтобы исключить возможность их дальнейшего восстановления или неправомерного использования, если иное не предусмотрено техническими особенностями информационных систем и требованиями законодательства.

10. Защита персональных данных

10.1. Компания принимает необходимые организационные, правовые и технические меры для защиты персональных данных от неправомерного доступа, раскрытия, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

10.2. Меры защиты персональных данных могут включать:

- ограничение доступа к персональным данным;
- разграничение прав доступа;
- применение паролей, средств идентификации и аутентификации;
- ведение журналов доступа и действий пользователей в информационных системах;
- резервное копирование данных;
- защиту от несанкционированного доступа;
- контроль действий пользователей информационных систем;
- заключение обязательств о конфиденциальности с работниками и подрядчиками;
- обучение работников правилам обработки и защиты персональных данных;
- внутренний контроль соблюдения правил обработки персональных данных;
- принятие мер по выявлению и предотвращению утечек персональных данных;
- системный ИТ-аудит;
- проверку соблюдения требований безопасности при передаче данных третьим лицам.

10.3. Конкретные технические меры защиты персональных данных определяются внутренними документами Компании, настройками информационных систем, требованиями информационной безопасности и характером обрабатываемых данных.

11. Инциденты, связанные с персональными данными

11.1. К инцидентам, связанным с персональными данными, относятся:

- утрата документов или файлов, содержащих персональные данные;
- ошибочная отправка персональных данных неуполномоченному лицу;
- несанкционированный доступ к информационной системе;
- раскрытие персональных данных третьим лицам без правового основания;
- уничтожение, изменение или блокирование персональных данных без законного основания;
- компрометация учетной записи работника;
- утечка персональных данных через электронную почту, мессенджеры, съемные носители или иные каналы;
- иные события, которые могут повлечь нарушение конфиденциальности или безопасности персональных данных.

11.2. Работник, выявивший инцидент или подозрение на инцидент, обязан незамедлительно сообщить об этом своему непосредственному руководителю, юридическому подразделению, службе безопасности и IT-подразделению.

11.3. При получении информации об инциденте Компания организует его первичную оценку, определяет характер и объем затронутых данных, возможные последствия, круг затронутых лиц, необходимые меры реагирования и порядок дальнейших действий.

11.4. По итогам рассмотрения инцидента могут приниматься следующие меры:

- ограничение или блокирование доступа;
- изменение паролей и средств аутентификации;
- восстановление данных из резервных копий;
- прекращение неправомерной передачи или обработки данных;
- уведомление заинтересованных лиц или органов, если это требуется законодательством;
- проведение служебной проверки;
- применение мер ответственности к виновным лицам;
- актуализация внутренних процедур и технических мер защиты.

12. Ответственность

12.1. Работники Компании несут ответственность за нарушение требований законодательства, настоящей Политики и иных внутренних документов Компании по вопросам обработки и защиты персональных данных.

12.2. Нарушением настоящей Политики признается, в том числе:

- обработка персональных данных без служебной необходимости;
- сбор избыточных персональных данных;
- передача персональных данных неуполномоченным лицам;
- раскрытие персональных данных без законного основания;
- использование персональных данных в личных целях;
- хранение персональных данных на личных устройствах без разрешения Компании;
- несоблюдение требований информационной безопасности;
- сокрытие факта инцидента, связанного с персональными данными;
- невыполнение законных требований субъекта персональных данных.

12.3. В зависимости от характера нарушения к виновным лицам могут применяться меры дисциплинарной, материальной, административной, гражданско-правовой или иной ответственности в соответствии с законодательством Республики Узбекистан и внутренними документами Компании.

13. Заключительные положения

13.1. Настоящая Политика вступает в силу с даты ее утверждения Правлением Компании и действует до ее отмены или замены новой редакцией.

13.2. Изменения и дополнения в настоящую Политику вносятся по решению уполномоченного органа Компании.

13.3. Настоящая Политика размещается в цифровых сервисах Компании и может быть предоставлена субъекту персональных данных по его запросу.

13.4. Вопросы, не урегулированные настоящей Политикой, регулируются законодательством Республики Узбекистан, договорами страхования, правилами страхования и внутренними документами Компании.

13.5. Контроль за исполнением настоящей Политики осуществляется руководителями структурных подразделений, юридическим подразделением, службой безопасности, IT-подразделением и иными ответственными лицами в пределах их компетенции.