Организация: Открытое акционерное общество «Государственная страховая организация»
Версия и дата: v1.0 / «_____» _____ **2025 года**
Утверждено: Председатель Правления Открытого акционерного общества «Государственная страховая организация», приказ № ___ от «» _____ 2025 года

КЫРГЫЗСКАЯ РЕСПУБЛИКА

КЫРГЫЗГОССТРАХ
ГОСУДАРСТВЕННАЯ СТРАХОВАЯ ОРГАНИЗАЦИЯ

Политика обработки персональных данных

Версия 1.0
Ответственные лица
Правление
Председатель Правления
Комплаенс-менеджер
Начальник IT- отдела

Версия	Дата	Изменение	Автор	Утверждение	Дата публикации
Версия 1.1					

Ссылка на исходный документ:

Этот документ является частью общей политики компании в области информационной безопасности и должен быть использован для обеспечения соблюдения внутренних стандартов безопасности.

Бишкек 2025

СОДЕРЖАНИЕ

Политика обработки персональных данных.
Регистрационный номер: 1–00045 - Реестр держателей (обладателей) массивов персональных данных

1. Общие положения

1.1. Настоящая Политика обработки персональных данных (далее — Политика) определяет порядок обработки персональных данных (ПДн) и меры по обеспечению их безопасности в ОАО «Государственная страховая организация» (далее — Держатель, ГСО) с целью защиты прав и свобод субъектов ПДн.
1.2. Политика распространяется на все операции с ПДн (автоматизированные и без), во всех ИС и на любых носителях, включая АИС 1С, Страхование, CRM/портал агентов и клиентов, корпоративную почту/офисные сервисы, систему видеомониторинга (в части видеозаписей, позволяющих идентифицировать лицо).
1.3. Политика доводится до работников и контрагентов, размещается на внутреннем портале/сайте ГСО.
1.4. Основные права и обязанности субъектов ПДн
1.4.1. Права субъектов ПДн:
a) на получение полной информации об их ПДн, обрабатываемых ГСО;
b) на доступ к своим ПДн, включая получение копии записей, содержащих их ПДн, за исключением случаев, предусмотренных законом;
c) на уточнение, блокирование или уничтожение ПДн, если данные неполные, устаревшие, неточные, получены незаконно или не нужны для заявленной цели;
d) на принятие предусмотренных законом мер по защите своих прав;
e) на иные права, предусмотренные законодательством Кыргызской Республики.
а) 1.4.2. Обязанности субъектов ПДн:
a) предоставлять ГСО достоверные данные о себе;
b) предоставлять документы, содержащие ПДн, в объёме, необходимом для заявленной цели (Приложение 1); своевременно сообщать об изменении своих ПДн.

1.5. Основные права и обязанности Держателя (ГСО)
1.5.1. Права ГСО:
a) получать от субъектов достоверные данные и документы, содержащие ПДн;
b) уточнять предоставленные субъектами ПДн в установленном порядке.

1.5.2. Обязанности ГСО:
a) обрабатывать ПДн в порядке, установленном законодательством;
b) рассматривать обращения субъектов по вопросам обработки ПДн в срок не более 15 (семи) календарных дней;
c) обеспечивать безвозмездный доступ субъектов к их ПДн;

d) принимать меры по актуализации ПДн;
e) обеспечивать защиту ПДн в соответствии с требованиями законодательства;
f) обеспечивать подписание субъектами и работниками обязательств о неразглашении ПДн (Приложение 2).

2. Объём и категории обрабатываемых ПДн

2.1. Категории субъектов ПДн: страхователи, выгодоприобретатели; застрахованные лица; заявители по страховым случаям; представители контрагентов, брокеров, агентов; сотрудники ГСО и кандидаты при трудоустройстве; подрядчики/поставщики/контрагенты (их уполномоченные лица).
2.2. Обрабатываемые ПДн (в зависимости от цели): Ф.И.О.; пол; дата и место рождения; гражданство; ПИН; адрес; телефон; e-mail; паспортные данные (серия, номер, кем/когда выдан); подпись; фотография/видеозапись (при пропускном режиме); образование, профессия, должность, стаж; семейное положение; сведения о членах семьи (при наличии правового основания); сведения о страховых договорах, премиях, выплатах и реквизитах оплаты (без хранения избыточных платёжных данных, не требуемых законом/договором); сведения о заработной плате и кадровые данные — для сотрудников; государственные/ведомственные награды — при наличии законного основания; технические данные онлайн-сервисов: файлы cookie, IP-адрес, геолокация (если включена пользователем).
2.3. Специальные категории ПДн обрабатываются только при наличии законного основания и необходимости для страхового продукта/выплаты: сведения о судимости (если прямо вытекает из условий продукта/закона); сведения медицинского характера (медицинские риски, страховые случаи по ДМС/НС и т.п.); биометрические/генетические данные — не обрабатываются, кроме случаев, прямо предусмотренных законом/договором.

3. Основные цели обработки ПДн

3.1. Заключение/исполнение/сопровождение договоров страхования/перестрахования; урегулирование убытков.
3.2. Исполнение требований по отчётности/налогам, ПОД/ФТ (идентификация, мониторинг, хранение сведений, выявление подозрительных операций, сообщения в уполномоченные органы) и KYC (идентификация, верификация, риск-профиль, периодическая актуализация).
3.3. CRM (учёт обращений и договоров, история взаимодействий, претензии, качество сервиса) и клиентский сервис.
3.4. Маркетинговые коммуникации по согласию (рассылки/оферты).

3.5. Кадровое администрирование, охрана труда, режим коммерческой тайны.
3.6. Пропускной режим/видеонаблюдение (зоны маркируются, информирование субъектов).

4. Правовая основа и нормативные ссылки

4.1. Политика разработана с учётом действующего законодательства Кыргызской Республики и международных требований в сфере защиты персональных данных и информационной безопасности, обязательных для ОАО «ГСО» как держателя (обладателя) массива персональных данных и оператора информационных систем.

4.2. Кодексы КР

a) **Цифровой кодекс Кыргызской Республики** *(вводится в действие Законом КР от 31.07.2025 № 179 по истечении шести месяцев со дня официального опубликования)* — базовый акт, регулирующий цифровые данные, электронное взаимодействие, требования к защите данных и ответственности участников.

b) **Гражданский кодекс КР (части I–II)** — общие положения о сделках, обязательствах и защите нематериальных благ, применимые к договорам страхования, обработке и защите персональных данных.

4.3. Законы КР

a) **Закон № 58 от 14.04.2008 «Об информации персонального характера»** — принципы и правовые основания обработки ПДн, права субъектов и обязанности держателя, требования к согласию, трансграничной передаче, безопасности и ответственности.

b) **Закон № 127 от 19.07.2017 «Об электронном управлении»** — организация электронного документооборота и взаимодействия с госорганами, требования к сервисам и их безопасности.

c) **Закон № 128 от 19.07.2017 «Об электронной подписи»** — правовой режим ЭП, порядок использования и признание юридической силы электронных документов при оформлении согласий, уведомлений и внутренних актов ГСО.

4.4. Подзаконные нормативные правовые акты

a) **Постановление Правительства КР № 760 от 21.11.2017** «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Устанавливает:

   a. уровни защищённости (*синий, зелёный, жёлтый, красный*) и порядок их определения на основе рейтинга угроз;

   b. критерии и методику оценки угроз (актуальность, вред, объём, содержание, продолжительность) и расчёт рейтинга;

c. обязательные организационно-технические меры безопасности по каждому уровню;
d. требования к журналированию, резервному копированию, контролю доступа, криптографической защите и оценке эффективности мер.

b) **Постановление Правительства КР № 762 от 21.11.2017** «Об утверждении требований по обеспечению безопасности информации в государственных информационных системах и при электронном взаимодействии». Закрепляет принципы ИБ, требования к организационным мерам (ответственные, внутренний контроль, обучение), техническим мерам (сегментация, МЭ/IDS/IPS, защита каналов, учёт инцидентов), управлению жизненным циклом ИС и мониторингу. Применяется ГСО постольку, поскольку ГСО взаимодействует с государственными ИС и использует электронное взаимодействие.

c) **Постановление Правительства КР № 200 от 11.04.2018 (в ред. № 296 от 17.06.2019)** «О порядке межведомственного электронного взаимодействия с использованием системы “Түндүк” и требованиях к информационным системам, участвующим во взаимодействии». Определяет требования к интеграциям ГСО с госорганами через «Түндүк»: защищённые каналы, аутентификация, авторизация, журналирование запросов и ответов, согласование форматов данных и управление инцидентами.

4.5. Ведомственные и методические документы

a) **Методика определения угроз безопасности в информационных системах персональных данных** (приказ уполномоченного госоргана по защите ПДн № 13-П от 19.12.2022) — обязательна для расчёта рейтинга угроз и выбора уровня защищённости; используется ГСО для документированного отнесения ИСПДн к уровню «красный».

4.6. Локальные нормативные акты ГСО

a) Настоящая Политика обработки ПДн.
b) **Положение об управлении доступом** (распределение ролей, RBAC, MFA, процедуры поднятия/снятия прав, ревизии доступа).
c) **Положение о криптографической защите** (алгоритмы, ключевая политика, хранение/ротация ключей, применение СКЗИ/TLS/VPN).
d) **Положение о журналировании и мониторинге** (состав логов, сроки хранения, защита от модификации, SIEM-корреляции, порядок анализа инцидентов).
e) **Политика резервного копирования и восстановления** (стратегия 3-2-1, тесты восстановления, RPO/RTO, хранение и шифрование бэкапов).
f) **Регламент реагирования на инциденты** (классификация, сроки уведомления, взаимодействие с уполномоченным органом, порядок расследования и RCA).

g) **Положение о взаимодействии с поставщиками** (требования к ИБ и ПДн в договорах, NDA, условия обработки/передачи ПДн, аудит поставщиков).
h) **Регламент защиты данных в АИС 1С, Страхование** (сегментация, журналирование, бэкапы, контроль изменений).
i) **Регламент эксплуатации системы видеомониторинга** (перечень камер и зон, сроки хранения, доступ по ролям, выдача копий по основаниям, защита видеоархивов).

4.7. Международные стандарты (применительно к лучшим практикам)

a) **ISO/IEC 27001:2022** — требования к системе менеджмента информационной безопасности (СМИБ): политика, оценка рисков, управление активами, инцидент-менеджмент, улучшение.
b) **ISO/IEC 27002:2022** — справочник средств контроля ИБ (контроль доступа, криптография, физическая безопасность, операционная безопасность, журналирование, поставщики, разработка и поддержка ИС). Применяются ГСО как ориентир для построения процессов и выбора мер, при этом приоритет имеют нормы законодательства КР и постановлений № 760/762/200.

5. Порядок и условия обработки ПДн

5.1. Обработка — автоматизировано/без автоматизации.
5.2. Операции: сбор, запись, систематизация, хранение, актуализация, использование, передача, блокирование, обезличивание, стирание, уничтожение.
5.3. Основания:
— согласие субъекта (бумажное/электронное с ЭП; цель, состав, срок, порядок отзыва — Приложении 1);
— договор (включая преддоговорные отношения, урегулирование);
— закон (в т.ч. ПОД/ФТ/KYC, учёт, отчётность, предписания регуляторов);
— законные интересы ГСО при соблюдении прав и свобод субъекта;
— иные случаи, предусмотренные НПА.
5.4. Прекращение обработки — при достижении цели, выявлении незаконной обработки, по требованию субъекта (если применимо) или по судебному акту.
5.5. Передача ПДн третьим лицам (банки-эквайеры, платёжные организации, брокеры, страховщики/перестраховщики, ИТ-подрядчики и др.) — по закону/договору и/или согласию, с обязательствами о конфиденциальности (см. форму в Приложении 2), только по защищённым каналам.
5.6. Трансграничная передача — при адекватной защите/международном основании/согласии; по защищённому каналу.

5.7. Хранение: минимально необходимый срок/по закону и правилам страхования; затем обезличивание/уничтожение актом.
5.8. Платёжные данные: без хранения избыточных реквизитов (полные PAN/CVV и пр.), токенизация платёжного провайдера, защищённые каналы и сегментация.

6. Оценка угроз безопасности ПДн

Методика: «Методика определения угроз безопасности в информационных системах персональных данных», приказ Агентства по защите ПДн № 13-П от 19.12.2022.

6.1. Классификация требований по уровням

Синий: доведение Политики; назначение ответственных; внутренний контроль; обязанности в ДИ/договорах; учёт носителей; протоколирование операций; ежедневные бэкапы.
Зелёный = Синий + проектирование ИС с учётом защиты; оценка эффективности мер до ввода/перед обновлениями; применение крипто средств.
Жёлтый = Зелёный + централизованное управление защитой ПДн; контроль помещений; неизменяемый электронный журнал; резервирование/НА ИС и журналов; автоматическое обнаружение/пресечение НСД и случайных изменений.
Красный = Жёлтый + только защищённые каналы; защита от утечек по тех каналам; сертифицированные СЗИ/ИС; ежегодный внешний аудит ИС и журнала.

6.2. Матрица угроз и расчёт уровня защищённости

Критерий	Балл	Обоснование
Актуальность угрозы	1	Интернет-доступ, «Түндүк», удалённые агенты, онлайн-платежи
Возможный вред субъекту	3	Финансовые/репутационные потери, риск мошенничества/утраты покрытия
Объём данных	3	Массовая база > 100 000 субъектов
Содержание данных	2	Спецкатегории, видеозаписи, идентификация личности
Продолжительность	1	Непрерывная обработка + архив

Итог: 1×3×3×2×1 = 18 баллов → «красный» уровень.

7. Требования к защите ПДн

7.1. Организационные меры

— Приказ о назначении Ответственного за ПДн/ИБ;

— RBAC, принцип «необходимости знать», учёт и контроль действий пользователей/админов;
— обучение/инструктажи, тестирование осведомлённости;
— классификация ИС и активов;
— план реагирования и регулярные учения;
— ежегодный внутренний аудит по Постановлению № 760.

7.2. Обязательные меры (по Требованиям)

a) принятием документа, определяющего политику держателя (обладателя) массива персональных данных в отношении обработки персональных данных, и доведением содержания данного документа до работников и контрагентов держателя (обладателя) массива персональных данных;

b) назначением лица (лиц), ответственных за обеспечение безопасности персональных данных при их обработке в информационных системах, и проведением их инструктажа по требованиям Закона Кыргызской Республики «Об информации персонального характера» и настоящих Требований;

c) осуществлением внутреннего контроля соответствия обработки персональных данных требованиям Закона Кыргызской Республики «Об информации персонального характера», настоящих Требований и иных документов, принятых по вопросам обработки персональных данных;

d) включением в трудовые договоры и должностные инструкции работников держателя (обладателя) массива персональных данных их обязанностей в отношении обработки персональных данных, а также положений о неукоснительном соблюдении Закона КР «Об информации персонального характера», настоящих Требований и иных документов;

e) ведением (на бумажном носителе или в электронном виде) журнала учёта машинных носителей персональных данных и списка лиц, в чьи должностные обязанности входит доступ к персональным данным;

f) при каждом вводе персональных данных в систему обработки данных, а также при их изменении или уничтожении — указанием лица, осуществившего ввод (изменение, уничтожение) данных, даты и времени операции;

g) созданием не реже одного раза в сутки резервной копии актуальных персональных данных, обрабатываемых в информационной системе персональных данных;

h) проектированием информационной системы и мер по её развитию с учётом характера обрабатываемых персональных данных и необходимости их защиты;

i) централизованным управлением системой защиты персональных данных, в том числе путём создания структурного подразделения, ответственного за реализацию настоящих Требований;

j) установлением системы контроля помещений, в которых установлена информационная система, позволяющей ограничить физический доступ к техническим средствам ИС только лицами с соответствующими полномочиями;
k) ведением автоматического электронного журнала (лога), фиксирующего все операции с персональными данными, с обеспечением невозможности внесения изменений в журнал задним числом;
l) обеспечением резервирования и высокой доступности в реальном времени информационной системы хранения и обработки персональных данных, а также автоматического электронного журнала, указанного выше;
m) наличием автоматической системы выявления и пресечения несанкционированного доступа к персональным данным, а также их случайного уничтожения или изменения;
n) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы и перед значительными обновлениями (расширениями) информационной системы, проводимой уполномоченным государственным органом по персональным данным и/или аккредитованными органами оценки соответствия;
o) применением шифровальных (криптографических) средств защиты информации, соответствующих техническим требованиям, для исключения несанкционированного доступа к персональным данным, их преднамеренного или случайного изменения либо уничтожения;
p) использованием только защищённых каналов связи при передаче персональных данных и (или) доступе к ним;
q) защитой персональных данных от утечек по техническим каналам;
r) применением средств защиты информации и/или информационных систем, прошедших в установленном порядке процедуру оценки соответствия в уполномоченном государственном органе по персональным данным и/или аккредитованном органе оценки соответствия;
s) регулярным (не реже одного раза в год) аудитом информационных систем держателя (обладателя) массива персональных данных и автоматического электронного журнала (лога), фиксирующего все операции с персональными данными, уполномоченным государственным органом по персональным данным и/или аккредитованным органом оценки соответствия.

8. Реагирование на инциденты

Пункт	Действие	Ключевые шаги	Сроки/требования	Артефакты/выходы
a)	Инициация и уведомление	Зафиксировать событие; уведомить Ответственного; при необходимости — регулятора и субъектов	Уведомление регулятора/субъектов ≤ **24 ч**	Запись о событии; журнал уведомлений

Пункт	Действие	Ключевые шаги	Сроки/требования	Артефакты/выходы
b)	Локализация и сдерживание	Блокировка учёток/ключей; изоляция хостов/сегментов; отключение интеграций; правила на NGFW/IDS/IPS	Немедленно (по приоритету инцидента)	Лист действий локализации
c)	Регистрация и доказательства	Открыть тикет в Реестре; собрать логи/SIEM/дампы/хеши; обеспечить неизменяемость (WORM/подпись)	Регистрация ≤ **1 ч**	Запись в Реестре; комплект артефактов
d)	Классификация и оценка воздействия	Присвоить уровень L1–L4; оценить объём и тип ПДн; оценить риски для субъектов и ГСО	Первичная оценка ≤ **2 ч**	Карта затронутых систем/ПДн; оценка риска
e)	Устранение и восстановление	Удалить артефакты; патчинг; ротация ключей/паролей; проверка целостности; восстановление из бэкапов (3-2-1)	Локализация ≤ **4 ч** (L4 — немедленно)	План исправлений; отчёт о восстановлении
f)	Коммуникации	Подготовить уведомление регулятору; при необходимости — субъектам; согласовать внешние сообщения	Формат по регламенту; язык — понятный	Текст уведомлений; рассылочные списки
g)	Закрытие и улучшение	Подготовить **RCA**; сформировать **CAPA-план** (меры/сроки/ответственные); обновить риск-оценку/процедуры	RCA ≤ **10 раб. дней** после закрытия	RCA; CAPA-план; обновлённые процедуры
h)	Документация и хранение	Вести Реестр инцидентов; хранить логи/отчёты/переписку/артефакты; ограничить доступ; обеспечить неизменяемость	Хранение материалов ≥ **12 месяцев**	Реестр; архив материалов расследования

9. Ответственность

Нарушители Политики и законодательства о ПДн несут дисциплинарную, административную или уголовную ответственность согласно праву КР и внутренним актам ГСО.

Приложение 1. Форма согласия субъекта ПДн

Город: _____ Дата: «» _____ 20 г.
Я, _____, (Ф.И.О., ПИН) даю согласие ОАО «ГСО» (адрес: _____) на обработку моих персональных данных.
Цель обработки: _____.
Состав ПДн: _____.
Срок обработки: до достижения цели и/или истечения установленных законом сроков хранения.
Права субъекта ПДн разъяснены. Настоящее согласие может быть отозвано путём направления письменного заявления/электронного документа, подписанного ЭП (электронную подпис).
Подпись _____ / Ф.И.О. _____

Приложение 2. Обязательство о неразглашении ПДн

Я, _____, (Ф.И.О., должность/основание доступа) обязуюсь не раскрывать и не использовать персональные данные, к которым получаю доступ при исполнении служебных/договорных обязанностей, соблюдать Политику ГСО и требования законодательства КР.
Срок действия обязательства: весь период доступа и 5 лет после его прекращения (если иное не установлено законом/договором).
Ответственность за нарушение мне разъяснена.
Подпись _____ Дата «» _____ 20 г.

Приложение 3. Реестр инцидентов (форма ведения)

№	Дата/время выявления	Система (1С, Страхование / CRM / видео / почта / сеть)	Тип инцидента	Краткое описание	Класс (L1–L4)	Принятые меры (локализация/устранение)	Ответственный	Статус	Дата/время закрытия	Примечания