СОГЛАШЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ

г. Алматы, Республика Казахстан
Версия №1 от 03.03.2026 года

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Конфиденциальная информация - любые сведения Исполнителя, прямо или косвенно раскрытые Заказчику, включая, но не ограничиваясь:
Бизнес-информация: бизнес-планы, стратегии развития, маркетинговые исследования, внутренние отчеты, планы по запуску продуктов, каналы продвижения, анализ рынка;
Финансовая информация: бухгалтерские отчеты, прогнозы, бюджетирование, расчет маржинальности, инвестиционные и кредитные планы, финансовые модели;
Клиентская и партнерская информация: базы данных, контактные данные, профили клиентов, персональные сведения, история взаимодействий, условия сделок, контракты;
Техническая и ИТ-информация: исходный код, алгоритмы, архитектура программных продуктов, модели ИИ, внутренние разработки, схемы баз данных, конфигурации IT-инфраструктуры;
Документация и регламенты: техническая документация, регламенты, инструкции, внутренние презентации, политики и процедуры безопасности, SLA, KPI, BPMN-карты процессов;
Любые сведения, явно обозначенные как конфиденциальные, а также любые сведения, доступные только ограниченному кругу лиц, включая устные и визуальные сведения, полученные через демонстрации, презентации, видеозаписи или удаленный доступ;
Дополнительные категории: ноу-хау, прототипы, идеи, концепции, стратегии монетизации, методы обучения ИИ, внутренние алгоритмы прогнозирования, результаты экспериментов и тестирований.
Конфиденциальная информация включает как существующую на момент подписания Соглашенияа информацию, так и сведения, которые могут быть созданы, модифицированы или раскрыты после даты подписания Соглашенияа.
1.2. *«Оператор»* - ТОО «Chatico», юридическое лицо, зарегистрированное на территории Республики Казахстан, БИН 251140012357, юридический адрес: город Алматы, проспект Назарбаева 65, офис 505; банковские реквизиты: АО "Народный банк Казахстана", ИИК KZ74601A861071779441, БИК HSBKKZKX, КБЕ 17; e-mail: support@chatico.ai, в лице директора Осипова Э.А.; администрирующее Сервис и обладающее исключительными правами на программное обеспечение и предоставляющее Пользователю доступ к ИИ-ассистенту Chatico на условиях Соглашения.
1.3. *Персональные данные* - любые сведения, относящиеся к идентифицируемым или идентифицируемым физическим лицам, включая сотрудников, клиентов, партнеров и подрядчиков, защищаемые:

- Законом РК «О персональных данных»;
- Законом РК «Об искусственном интеллекте» в части обработки персональных данных;
- локальными внутренними регламентами Исполнителя по защите персональных данных.

Персональные данные включают, но не ограничиваются: ФИО, идентификационные номера, контактные данные, электронные адреса, учетные записи в системах, финансовую информацию, историю взаимодействий и любые другие сведения, позволяющие прямо или косвенно идентифицировать лицо.
1.4. *Результаты* - любые продукты, отчеты, документы, алгоритмы, модели ИИ, прогнозы, аналитические и вычислительные материалы, созданные Заказчиком на основе Конфиденциальной информации, включая промежуточные версии, прототипы и тестовые данные.
1.5. *Конкурентное использование* - любое использование Конфиденциальной информации или Результатов, включая:

- создание, запуск или продвижение товаров, услуг или сервисов, конкурирующих с Исполнителем;
- передачу информации конкурентам или третьим лицам с целью получения выгоды;
- использование данных для разработки собственных моделей ИИ, аналитических инструментов или алгоритмов, аналогичных разработкам Исполнителя.

1.6. *Недобросовестный партнер* - любое физическое или юридическое лицо, которое:

- действует с целью обмана, кражи, обхода обязательств, нарушения условий Соглашенияа;
- причиняет ущерб Исполнителю или его Заказчикам;
- раскрывает Конфиденциальную информацию третьим лицам без согласия Исполнителя;
- совершает любые действия, прямо или косвенно направленные на подрыв деловой репутации или конкурентоспособности Исполнителя;
- нарушает положения о персональных данных, интеллектуальной собственности и правах на результаты.

Факт недобросовестности устанавливается на основании документально подтвержденных обстоятельств, включая журналы активности, акты аудита, заключения экспертов, судебные решения и иные допустимые доказательства.
1.7. *Информационные системы* - все цифровые, облачные, локальные и гибридные платформы, включая, но не ограничиваясь: CRM, ERP, PIM, BI-системы, системы аналитики и отчетности, облачные хранилища и платформы обработки данных, локальные серверы, базы данных, файловые хранилища, инструменты для работы с ИИ, алгоритмами, моделями прогнозирования и аналитики, любые устройства и системы, использующие Конфиденциальную информацию для хранения, обработки, передачи или визуализации. Любая работа с информационными системами должна соответствовать требованиям информационной безопасности, включая шифрование, двухфакторную аутентификацию, журналирование и контроль доступа.
1.8. *Форс-мажор* - обстоятельства непреодолимой силы, включая: природные и техногенные катастрофы (землетрясения, наводнения, пожары, аварии на коммуникациях); отключение электроэнергии или сетевых ресурсов, включая интернет и телекоммуникации; кибератаки, взломы, вирусные и вредоносные воздействия; действия государственных органов, включая ограничения, запреты, расследования; другие непредвиденные обстоятельства, которые делают невозможным выполнение обязательств Сторонами. При наступлении форс-мажора Стороны обязаны

немедленно уведомить друг друга и принять все разумные меры для минимизации последствий, при этом обязанности по защите Конфиденциальной информации сохраняются полностью.

2. ОБЯЗАТЕЛЬСТВА СТОРОН

2.1. Стороны обязуются:

- Использовать Конфиденциальную информацию исключительно в рамках целей настоящего Соглашенияа и строго в интересах Исполнителя. Любое отклонение от целей Соглашенияа признается нарушением и влечет гражданско-правовую ответственность, а при наличии состава правонарушения - ответственность, предусмотренную законодательством Республики Казахстан.
- Применять современные стандарты информационной безопасности и управления рисками, внедрять шифрование данных, двухфакторную аутентификацию и безопасное хранение резервных копий.
- Немедленно уведомлять Исполнителя о любых подозрительных действиях, попытках несанкционированного доступа, утечки информации, кибератак или других инцидентах информационной безопасности.
- Не использовать Конфиденциальную информацию для конкурентной деятельности, обхода условий Соглашенияа, получения личной выгоды или передачи третьим лицам без письменного согласия Исполнителя.
- Обеспечивать физическую защиту документов и оборудования, содержащего Конфиденциальную информацию, а также цифровую защиту всех электронных данных, включая серверы, облачные сервисы и устройства сотрудников.
- Немедленно предпринимать меры по локализации инцидентов и устранению последствий утечек, включая уведомление правоохранительных органов при угрозе ущерба.

2.2. Заказчик обязуется:

- Ограничивать доступ к Конфиденциальной информации исключительно уполномоченным сотрудникам, прошедшим проверку на благонадежность и сертификацию по информационной безопасности.
- Обеспечивать подписание настоящего NDA и внутренних регламентов безопасности всеми сотрудниками, имеющими доступ к информации, а также подрядчиками и субподрядчиками.
- Запрещать копирование, распространение, хранение и обработку информации вне согласованных информационных систем, включая локальные устройства, флеш-накопители и личные облачные сервисы.
- По первому требованию Исполнителя немедленно возвращать все материалы, безопасно уничтожать электронные и физические копии с предоставлением доказательств (скриншоты, акты уничтожения, отчеты BI-системы), блокировать доступ сотрудников к информации.
- Вести журнал всех действий с данными, включая доступ, копирование, удаление, передачу и обработку, с возможностью предоставления Исполнителю подробного отчета в течение 24 часов.
- Немедленно информировать Исполнителя о любом инциденте, включая попытку утечки, вмешательство третьих лиц, кражу устройств или подозрительную активность.
- Обеспечивать постоянный мониторинг безопасности, включая антивирусную защиту, обновление ПО и контроль целостности данных.

При нарушении Заказчиком настоящих обязательств компенсирует все прямые и косвенные убытки, включая упущенную выгоду, судебные расходы и расходы на аудит и восстановление данных.

2.3. Исполнитель обязуется:

- Обеспечивать защиту Конфиденциальной информации на всех этапах передачи, хранения и обработки, используя современные технологии шифрования и контроля доступа.
- Информировать Заказчика о правилах безопасного хранения, передачи и обработки информации, включая инструкции по использованию электронных систем и облачных платформ.
- Предоставлять техническую поддержку, консультации и необходимые инструменты для безопасной работы с информацией, включая удаленный контроль доступа и мониторинг действий сотрудников Заказчика.
- В случае выявления нарушения со стороны Заказчика - немедленно предпринимать меры по ограничению доступа и блокировке действий, включая автоматизированные механизмы BI-систем.

2.4. Исполнитель имеет право проводить регулярный и внеплановый аудит IT-систем, журналов доступа, документации и всех действий Заказчика, включая использование облачных сервисов и локальных устройств. Любое нарушение условий доступа к Конфиденциальной информации считается основанием для немедленной автоматической блокировки аккаунтов и устройств, временной или постоянной приостановки сотрудничества, взыскания компенсации ущерба. Аудит может проводиться как дистанционно (с использованием BI-систем, логирования и мониторинга), так и на объекте Заказчика. Аудит осуществляется исключительно в части, связанной с обработкой Конфиденциальной информации Исполнителя, без вмешательства в коммерческую тайну Заказчика, не связанную с предметом Соглашенияа. Все выявленные нарушения фиксируются в официальных актах, которые имеют юридическую силу в судах РК и могут использоваться для немедленных претензионных и судебных действий. Заказчик компенсирует все прямые и косвенные убытки, включая расходы на восстановление и защиту информации, упущенную выгоду, судебные издержки и услуги независимых экспертов.

3. ИСКЛЮЧЕНИЯ ИЗ КОНФИДЕНЦИАЛЬНОСТИ

3.1. Конфиденциальная информация не считается таковой, если:

3.1.1. *Общедоступность* - сведения стали общедоступными исключительно без нарушения настоящего Соглашенияа, включая публикации в СМИ, официальных базах данных или общедоступных источниках. Доступность информации по инициативе Заказчика, его сотрудников, партнеров или третьих лиц без письменного согласия Исполнителя не снимает ответственности за нарушение.

3.1.2. *Законное получение* - сведения получены Заказчиком законным образом от третьих лиц, при условии, что такие третьи лица не обязаны сохранять их в тайне и не нарушают закон. Заказчик обязан документально подтвердить

источник и правомерность получения.
3.1.3. *Раскрытие по закону* - информация может быть раскрыта только при наличии обязательного требования закона, судебного решения или постановления уполномоченного органа, при этом:
- Заказчик обязан немедленно уведомить Исполнителя о полученном требовании;
- раскрытие должно быть минимально возможным для выполнения закона;
- любая передача информации третьим лицам в рамках закона должна фиксироваться документально, с сохранением доказательств уведомления Исполнителя;

Заказчик несет ответственность за любые последствия превышения объема раскрытия.
3.2. Любое использование, копирование, распространение, декомпиляция, обратное проектирование, публикация или иное обращение с Конфиденциальной информацией, не связанное с целями Соглашенияа, считается грубым нарушением и является основанием для:
- взыскания 100% фактически понесенных убытков, включая упущенную выгоду;
- штрафных санкций, предусмотренных Соглашениями или отдельным письменным соглашением Сторон;
- применения запретительных судебных мер, включая приказы о немедленной блокировке систем, изъятии материалов и запрете действий Заказчика;
- привлечения к уголовной или административной ответственности при выявлении факта промышленного шпионажа, кражи данных, нарушения закона о персональных данных, об ИИ или иного законодательства РК.

3.3. Заказчик обязан немедленно прекратить любые действия, которые могут привести к нарушению условий настоящего раздела, и предоставить Исполнителю письменное подтверждение прекращения таких действий.
3.4. Исполнитель вправе самостоятельно или через доверенных лиц проводить проверку всех систем, каналов связи и хранения данных Заказчика для выявления нарушения. Нарушение фиксируется как доказательство для взыскания убытков и применения санкций.
3.5. Любое превышение объема раскрытия информации, указанного в пп. 3.1.3 Соглашенияа, или попытка использовать информацию, не подпадающую под конфиденциальность, трактуется как преднамеренное нарушение Соглашенияа, что усиливает правовые последствия для Заказчика.

4. ПРАВА И ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ

4.1. Исключительные права Исполнителя:
4.1.1. Все права, включая исключительные права на Результаты, алгоритмы, исходный код, модели ИИ, базы данных, техническую документацию, методики, визуализации, отчеты, аналитические материалы и любую интеллектуальную собственность, созданную Исполнителем или совместно, полностью принадлежат Исполнителю.
4.1.2. Заказчик признает, что любая разработка, модификация или адаптация Результатов в рамках настоящего Соглашенияа не передает права на интеллектуальную собственность, кроме лицензии, специально оговоренной в п.4.2 Соглашения.
4.2. Лицензия для Заказчика
4.2.1. Заказчик получает ограниченную, неисключительную, непередаваемую, отзывную лицензию на использование Результатов исключительно для внутренних целей, строго в рамках настоящего Соглашенияа.
4.2.2. Заказчик не имеет права предоставлять доступ к Результатам третьим лицам без письменного согласия Исполнителя, включая аутсорсинговые компании, подрядчиков и дочерние организации.
4.2.3. Использование лицензии ограничивается сроком действия Соглашенияа и может быть немедленно прекращено в случае нарушения условий Соглашенияа, попыток передачи, копирования или адаптации Результатов.
4.3. Запрещенные действия и использование:
4.3.1. Заказчик обязуется не использовать Результаты для создания конкурирующих сервисов, разработки аналогичных продуктов, публикаций или передачи третьим лицам в любой форме.
4.3.2. Любая попытка обратного проектирования, декомпиляции, копирования, адаптации, модификации, публикации, воспроизведения или внедрения Результатов в сторонние системы считается нарушением Соглашенияа.
4.3.3. Заказчик обязуется не внедрять Результаты в собственные ИТ-системы, облачные сервисы или модели ИИ без письменного разрешения Исполнителя.
4.4. Санкции за нарушение прав:
4.4.1. Любое нарушение прав интеллектуальной собственности Исполнителя является основанием для немедленной блокировки доступа Заказчика к Результатам, информационным системам и внутренним ресурсам.
4.4.2. Заказчик несет полную материальную ответственность за ущерб, включая прямые убытки, упущенную выгоду, судебные расходы, расходы на экспертизы и восстановление интеллектуальной собственности.
4.4.3. Исполнитель вправе потребовать немедленного удаления, уничтожения или возврата всех Результатов, включая копии, коды, модели ИИ и базы данных, независимо от способа хранения (цифровое, физическое или облачное).
4.5. Дополнительные обязательства Заказчика:
4.5.1. Заказчик обязуется применять все необходимые меры защиты Результатов: шифрование, контроль доступа, двухфакторную аутентификацию, журналы доступа и безопасное хранение данных.
4.5.2. Заказчик обязуется уведомлять Исполнителя о любых попытках третьих лиц получить доступ к Результатам или использовать их в обход условий Соглашенияа.
4.5.3. Заказчик обязуется подписывать NDA со всеми сотрудниками и подрядчиками, которые имеют доступ к Результатам.
4.5.4. Заказчик несет ответственность за действия своих сотрудников, подрядчиков и любых лиц, имеющих доступ к Результатам.
4.6. Право Исполнителя на судебную защиту:
4.6.1. Исполнитель вправе обращаться в суд или государственные органы с требованием о запрете использования Результатов, взыскании убытков и применении обеспечительных мер без предварительного уведомления.

4.6.2. Исполнитель вправе применять автоматические меры защиты (блокировка учетных записей, дистанционная деактивация доступа к программным продуктам и ИТ-ресурсам).

5. ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ИИ

5.1. Стороны обязуются строго соблюдать:

- Закон РК «О персональных данных» (№ 94-V ЗРК);
- Закон РК «Об искусственном интеллекте» (№ 288-VI ЗРК);
- Международные стандарты защиты данных, включая GDPR, ISO 27001 и NIST, в части, не противоречащей законодательству РК^ прошедшим внутреннее обучение по информационной безопасности либо обучение, соответствующее общепринятым стандартам защиты информации.

5.1.2. Стороны обязуются обеспечить внедрение и поддержание всех организационных и технических мер защиты персональных данных и данных, используемых в ИИ, включая шифрование данных в состоянии покоя и при передаче, двухфакторную аутентификацию и контроль доступа по ролям, журналирование всех операций с данными с возможностью аудита, регулярное резервное копирование и хранение данных в защищенных облачных или локальных системах.

5.1.3. Стороны обязуются незамедлительно уведомлять друг друга о любых инцидентах, связанных с утечкой, компрометацией или несанкционированным доступом к персональным данным или данным ИИ, и совместно предпринимать меры по минимизации ущерба.

5.2. Заказчик обязуется:

- не передавать, не раскрывать и не использовать персональные данные и данные ИИ третьим лицам без письменного согласия Исполнителя;
- хранить и обрабатывать данные с использованием современных методов защиты, включая шифрование, контроль доступа по ролям, VPN и безопасные каналы передачи данных;
- обеспечивать аутентификацию всех пользователей и регистрацию их действий в системе;
- уничтожать, анонимизировать или возвращать данные по первому требованию Исполнителя в безопасной форме с письменным подтверждением;
- не использовать персональные данные и данные ИИ для создания, обучения или оптимизации собственных моделей ИИ или алгоритмов без письменного согласия Исполнителя;
- проводить регулярное обучение и инструктаж сотрудников по вопросам защиты персональных данных и конфиденциальной информации;
- при работе с персональными данными Клиентов и сотрудников Исполнителя использовать только согласованные и одобренные Исполнителем системы обработки данных.

Заказчик несет полную материальную, юридическую и репутационную ответственность за любое нарушение вышеуказанных требований, включая: прямой и косвенный ущерб, упущенную выгоду, расходы на судебные разбирательства и независимые экспертизы.

5.3. Любое нарушение правил обработки персональных данных и данных ИИ считается серьезным нарушением Соглашенияа и приводит к:

- немедленной автоматической блокировке доступа Заказчика к системам и данным Исполнителя;
- штрафу в размере 1 000 000 KZT за каждый случай нарушения;
- обязательной компенсации всех убытков Исполнителя, включая упущенную выгоду, расходы на восстановление данных, проведение экспертиз и судебные издержки;
- при необходимости - уведомлению правоохранительных органов и инициированию уголовного расследования в соответствии с законодательством РК;
- возможности Исполнителя расторгнуть Соглашения в одностороннем порядке без предварительного уведомления и без возмещения любых средств Заказчику.

5.3.2. Заказчик обязуется возместить ущерб Исполнителя и третьих лиц, причиненный в результате несанкционированного раскрытия персональных данных или использования данных ИИ.

5.4. Права Исполнителя на использование данных:

5.4.1. Исполнитель вправе использовать анонимизированные или агрегированные данные для:

обучения и совершенствования моделей ИИ;

аналитики и прогнозирования;

улучшения продуктов и услуг, предоставляемых Исполнителем;

публикаций в научных и исследовательских материалах, при условии полной анонимизации данных.

5.4.2. Исполнитель имеет право без согласия Заказчика хранить и обрабатывать персональные данные и данные ИИ в целях обеспечения непрерывной работы систем, выявления нарушений, проведения аудита и повышения уровня безопасности.

5.4.3. Любое использование персональных данных или данных ИИ Заказчика для иных целей, кроме анонимизированного анализа и законных целей Исполнителя, запрещено.

5.5. Исполнитель имеет право проводить плановые и внеплановые аудиты соблюдения Заказчиком требований по обработке персональных данных и данных ИИ.

5.6. Нарушение правил аудита, попытка сокрытия инцидентов или вмешательства в систему мониторинга - считается прямым нарушением Соглашенияа с последствиями, описанными в разделе 5.3 Соглашенияа.

6. ОТВЕТСТВЕННОСТЬ И САНКЦИИ

6.1. Нарушение условий Соглашенияа Заказчиком влечет полную материальную, административную и уголовную ответственность в пределах, установленных законодательством РК, включая:

- прямой ущерб (финансовые потери, утрату активов, репутационные риски);

- косвенный ущерб (упущенную выгоду, потерю клиентов, снижение доходов);
- компенсацию всех расходов Исполнителя на восстановление безопасности и устранение последствий нарушения;
- возмещение расходов на аудит, экспертизы, услуги юристов и судебные издержки.

Любое нарушение, умышленное или по неосторожности, считается основанием для взыскания 100% фактических и документально подтвержденных убытков, включая потери от конкурентного использования информации.

6.2. Фиксированные штрафы за конкретные нарушения:

- 500 000 KZT - за любую несанкционированную утечку информации, включая электронные, бумажные и устные каналы;
- 2 000 000 KZT - за использование Конфиденциальной информации или Результатов в конкурентных целях, включая косвенные действия через третьих лиц;
- 1 000 000 KZT - за обход блокировок, попытки удаленного или физического доступа к информационным системам Исполнителя, включая VPN, прокси, обход двухфакторной аутентификации;
- компенсация всех судебных расходов, экспертиз, процедур по восстановлению данных и программного обеспечения, включая расходы на привлечение сторонних специалистов и консультантов.

6.3. Любое раскрытие информации конкурентам, клиентам или третьим лицам рассматривается как умышленное нарушение и влечет:

- немедленную блокировку доступа Заказчика к информационным системам и материалам;
- Заказчик обязан возместить убытки в полном объеме;
- право Исполнителя инициировать немедленные судебные или административные меры, включая обеспечение доказательной базы через BI-систему и журналы активности;
- обязанность Заказчика полностью компенсировать любые репутационные и деловые потери Исполнителя.

6.4. Заказчик не имеет права использовать Результаты или Конфиденциальную информацию без проверки компетентным специалистом, утвержденным Исполнителем, если иное не согласовано Сторонами письменно. Любое несанкционированное использование влечет ответственность Заказчика за все последствия, включая ущерб третьим лицам, технические сбои и убытки Исполнителя. Заказчик обязан уведомлять Исполнителя о любых действиях с Результатами до их использования, иначе действия признаются нарушением Соглашенияа.

6.5. Заказчик обязан заключить страховой Соглашения на случай:

- утечки конфиденциальной информации;
- конкуренции и недобросовестного использования данных;
- кибератак, взлома систем, потери данных;
- ответственности перед третьими лицами.

6.6. Страховая сумма должна покрывать полный спектр потенциального ущерба, включая судебные расходы, восстановление данных и репутационные потери. Несоблюдение этого требования является основанием для немедленного приостановления работы Заказчика с системами Исполнителя до момента подтверждения страхования. Исполнитель вправе фиксировать все действия Заказчика в автоматизированных журналах и использовать их как доказательства в суде. Любое нарушение фиксируется в системе BI и блокируется доступ до решения Исполнителя. Заказчик несет полную ответственность за любые попытки манипулирования журналами активности или подделки данных.

6.7. Стороны признают установленные настоящим Соглашением штрафы и неустойки разумными, соразмерными возможным последствиям нарушения, учитывая цифровой характер информации, риски конкурентного использования, утраты коммерческой тайны и репутационные последствия. Уплата штрафа не освобождает Заказчика от обязанности возместить убытки в части, превышающей сумму штрафа. Стороны подтверждают, что размер штрафа определен с учетом цифрового характера информации, рисков утраты коммерческой тайны и является экономически обоснованным.

7. АВТОМАТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ

7.1. Любое обнаруженное нарушение, попытка несанкционированного доступа, копирования, скачивания, передачи, раскрытия или обхода защиты Конфиденциальной информации инициирует немедленную автоматическую блокировку всех учетных записей Заказчика, связанных с Исполнителем. Система фиксирует: IP-адрес, геолокацию, устройство, время действия и характер нарушения. Фиксированные журналы действий являются юридически допустимыми доказательствами в судах Республики Казахстан и международных юрисдикциях.

7.2. Заказчик обязуется не пытаться обойти блокировку, не использовать альтернативные устройства, VPN, прокси, клоны учетных записей или другие методы обхода. Нарушение обязательств автоматически влечет:

- штраф 1 000 000 (один миллион) тенге;
- компенсацию всех убытков, включая упущенную выгоду, судебные и экспертные расходы;
- автоматическую приостановку любых дальнейших взаимодействий до полного устранения нарушения.

Стороны признают указанные штрафы разумными и соразмерными потенциальному ущербу, учитывая характер информации и цифровые риски.

7.3. Все действия, связанные с акцептом документов, согласий и подтверждений Заказчика, осуществляются через eID РК, которая признается юридически эквивалентной подписи в соответствии с законодательством Республики Казахстан. Стороны признают электронные журналы, логи систем, BI-отчеты и данные eID допустимыми доказательствами в судах Республики Казахстан в соответствии с законодательством о цифровых документах.

7.4. При выявлении угрозы утечки, кражи или несанкционированного использования информации Исполнитель вправе направить материалы в правоохранительные органы (при необходимости). Исполнитель имеет право немедленно применять временные запретительные меры, включая блокировку доступа, приостановку исполнения договорных обязательств и предотвращение передачи данных третьим лицам.

7.5. Все действия Заказчика фиксируются в BI-системе Исполнителя с развернутыми отчетами: время, тип операции, результат, пользователь, система. Эти данные формируют автоматическую доказательственную базу для суда, используются для оценки ущерба, расчета штрафов и компенсаций, позволяют проводить автоматический аудит по требованиям ISO 27001 и внутренним регламентам.
7.6. Любая попытка обхода защиты, вмешательства в BI-систему, эмуляции eID, кибератаки или манипуляций с журналами действий Заказчика рассматривается как серьезное нарушение Соглашенияа, влечет увеличение штрафа до 5 000 000 (пять миллионов) тенге, а также взыскание всех документированных убытков, если иное не будет определено судом с учетом характера нарушения. Заказчик обязуется компенсировать Исполнителю стоимость судебной экспертизы, аудита, восстановления данных и репутационные потери, вызванные нарушением. Исполнитель оставляет за собой право немедленного разрыва Соглашенияа без предупреждения и подачи исков в гражданском, административном и уголовном порядке при попытке злонамеренного обхода мер защиты.

8. СРОК ДЕЙСТВИЯ И ПОСТКОНТРАКТНЫЕ ОБЯЗАТЕЛЬСТВА

8.1. Соглашения вступает в силу с даты подписания Сторонами либо электронного акцепта через eID и действует в течение всего периода сотрудничества.
8.2. Обязательства по сохранению коммерческой тайны действуют до момента ее законного раскрытия или утраты коммерческой ценности.
8.3. Срок исковой давности по требованиям Исполнителя исчисляется с момента обнаружения нарушения в соответствии с положениями Гражданского кодекса Республики Казахстан.
8.4. Наличие утечки в период доступа Заказчика к информации создает обоснованное предположение его ответственности до представления доказательств отсутствия вины.
8.5. Исполнитель вправе проводить аудит соблюдения обязательств даже после прекращения Соглашенияа.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящий Соглашения регулируется законодательством Республики Казахстан, включая Гражданский кодекс РК, Закон «О персональных данных», Закон «Об искусственном интеллекте» и иные применимые нормативные акты. В случае противоречий применяются императивные нормы законодательства Республики Казахстан.
9.2. Все уведомления и требования по Соглашению должны направляться письменно, по электронной почте с подтверждением доставки или через официальные системы eID, PIM/CRM или BI-платформу, фиксирующую факт получения. Уведомления считаются доставленными с момента подтверждения получения или фиксации в системе.
9.3. Любые изменения, дополнения или корректировки Соглашенияа действительны только при письменном согласии обеих Сторон, оформленном на бумаге или с использованием eID. Устные договоренности или действия, противоречащие письменно оформленным условиям, не имеют юридической силы.
9.4. Любое нарушение, совершенное умышленно, с целью конкурентного использования информации либо обхода мер защиты, признается существенным нарушением Соглашенияа и освобождает Исполнителя от обязанности предварительного уведомления перед применением обеспечительных мер.
9.5. Подписи Сторон, включая акцепт через eID, имеют равную юридическую силу с подписанием на бумажном носителе. Соглашения признается полностью исполненным и юридически действительным после подписания обеими Сторонами или акцепта через eID. Заказчик подтверждает, что ознакомлен с положениями о постконтрактных обязательствах, ответственности и порядке контроля исполнения Соглашенияа, и обязуется строго их соблюдать.
9.6. Все споры, разногласия и требования, возникающие из настоящего Соглашенияа, подлежат рассмотрению в судебных органах Республики Казахстан по месту регистрации Исполнителя.