

Privacy Policy

Introduction

Вітаємо у використанні продуктів і послуг Agent X Group LLC. Ця Політика конфіденційності («Політика») пояснює, як обробляються персональні дані під час доступу та використання вебсайтів, застосунків, клієнтів, API, інтеграцій, плагінів, SDK та інших технологічних інтерфейсів і форм-факторів (разом — «Послуги»). Послуги є технологічно нейтральними інструментами і не визначають цілі використання користувачами у зовнішніх середовищах .

Будь ласка, уважно прочитайте цю Політику перед початком використання Послуг. Продовження доступу або використання, а також дії на кшталт «погоджуюсь», реєстрації, завантаження, встановлення чи входу означають, що Політика прочитана та прийнята, у тому числі згода на обробку необхідних категорій персональних даних для надання базових і додаткових функцій, як це описано нижче. Якщо положення є неприйнятними, слід припинити використання Послуг .

Договірна інтеграція. Ця Політика є невід'ємною частиною Умов користування Agent X Group LLC. У випадку суперечностей між цими документами, застосовуються положення, що забезпечують надання Послуг при дотриманні вимог захисту даних; положення про відмову від гарантій та обмеження відповідальності з Умов користування поширюються на цю Політику в максимально дозволених законом межах .

Ролі за GDPR. Залежно від функції обробки:

- Контролер: Agent X Group LLC діє як контролер там, де самостійно визначає цілі та засоби обробки (наприклад, білінг, безпека, ведення облікових записів, аналітика, комунікації) .
- Процесор: Agent X Group LLC діє як процесор, коли обробляє дані від імені клієнта для функцій, які клієнт ініціює і контролює (наприклад, синхронізація профілів, командний доступ, робочі простори, інтеграції). У цих випадках клієнт є контролером і відповідає за правові підстави, належні повідомлення суб'єктам даних і виконання їхніх прав .

Згода та інші правові підстави. Там, де згода є необхідною, вона надається явним способом через інтерфейси або налаштування облікового запису та може бути відкликана у будь-який час з майбутнім ефектом через відповідні механізми. В інших випадках обробка може базуватися на виконанні договору, законному інтересі, юридичних зобов'язаннях або захисті життєво важливих інтересів, залежно від контексту, як це детально описано в окремих розділах Політики .

Оновлення Політики. Політика може періодично змінюватися шляхом публікації оновленої версії в Послугах без окремого попередження. Продовження використання після публікації змін означає згоду з оновленою Політикою; у разі незгоди обробку можна обмежити або припинити використання Послуг через налаштування або видалення облікового запису .

Географічна дія. Ця Політика застосовується до обробки даних незалежно від місця знаходження користувача; для резидентів ЄЄЗ/Великої Британії/Швейцарії, Каліфорнії та інших юрисдикцій з особливими вимогами окремі розділи містять додаткові відомості про права та вимоги локального законодавства .

Контактні канали. Питання щодо цієї Політики або реалізації прав суб'єктів даних можна надсилати за адресою office@agentx.company або через призначені канали підтримки у Послугах. Канали можуть змінюватись із часом у технологічно нейтральний спосіб .

I. Scope

Охоплення Політики. Ця Політика застосовується до обробки персональних даних у зв'язку з використанням продуктів і послуг Agent X Group LLC, що надаються через вебсайти, програмні клієнти, мобільні застосунки, веб- і десктопні інтерфейси, API, інтеграції, плагіни, SDK, а також інші поточні або майбутні технологічні канали та фактори, які можуть з'являтися внаслідок розвитку технологій (разом — «Послуги») .

Технологічна нейтральність. Послуги є технологічно нейтральними інструментами; визначення цілей і способів використання у зовнішніх середовищах (наприклад, на сторонніх платформах) не контролюється Agent X Group LLC, і відповідальність за таке використання несе користувач або відповідний контролер даних, залежно від контексту .

Винятки. Ця Політика не застосовується до продуктів/послуг партнерів або інших третіх сторін, навіть якщо вони інтегровані чи доступні через Послуги (наприклад, сторонні розширення, маркетплейси, платіжні провайдери, хмарні сервіси). Такі сервіси регулюються власними політиками конфіденційності та умовами, із якими слід ознайомитися окремо .

Ролі сторін. Коли Agent X Group LLC обробляє дані від імені клієнта в межах функцій, що ініціюються/контролюються клієнтом, Agent X Group LLC діє як процесор, а клієнт — як контролер. Якщо Agent X Group LLC самостійно визначає цілі та засоби обробки (наприклад, білінг, безпека, аналітика), вона діє як контролер; у такому разі цю Політику слід читати разом із Умовами користування та відповідними політиками Agent X Group LLC .

Територіальна дія. Політика застосовується до обробки даних незалежно від місцезнаходження користувача; додаткові повідомлення можуть застосовуватися до резидентів ЄЄЗ/ВБ/Швейцарії, Каліфорнії та інших юрисдикцій з особливими вимогами .

II. Data Collection and Use

Загальні принципи. Під час використання Послуг може здійснюватися збір і обробка персональних даних для надання базових і додаткових функцій. Категорії даних, цілі, правові підстави, строки зберігання та налаштування контролю залежать від обраних модулів, інтеграцій і тарифного плану, а також від ролі Agent X Group LLC як контролера або процесора в конкретному контексті .

Базові функції (необхідні дані). Для запуску облікового запису, автентифікації, білінгу, безпеки, підтримки, забезпечення працездатності клієнтів, синхронізації критично необхідних параметрів середовища та виконання договору потрібні певні дані. Відмова надати такі дані може зробити неможливим доступ або використання базових функцій Послуг .

Додаткові функції (опційні дані). Окремі розширені можливості — наприклад, командний доступ і спільний простір, інтеграції з третіми сторонами, аналітичні панелі, маркетингові розсилки за згодою, телеметрія покращення продуктивності, бета-функції — можуть потребувати додаткових даних. Згода на такі обробки є добровільною і може бути

надана/відкликана через налаштування; відмова не впливає на доступ до базових функцій, однак може обмежити або змінити роботу відповідних додаткових модулів .

Варіативність модулів. Оскільки набір функціональних модулів і інтеграцій відрізняється між користувачами, конкретні категорії даних і обсяг обробки можуть відрізнятися. Детальні описи доступні у відповідних інтерфейсах модулів і довідкових матеріалах у Послугах; під час активації конкретної функції відображаються актуальні відомості про категорії даних, цілі, правові підстави та налаштування контролю .

Правові підстави. Обробка базових даних здійснюється переважно для виконання договору, дотримання правових зобов'язань і забезпечення безпеки/цілісності сервісу; для опційних обробок може використовуватись згода або законний інтерес із проведенням тесту балансування інтересів та наданням механізмів заперечення, якщо застосовно. Для сценаріїв, де Agent X Group LLC діє як процесор, правову підставу визначає контролер (клієнт) і забезпечує належні повідомлення суб'єктам даних .

Мінімізація та пропорційність. Збір і використання даних обмежуються тим, що є необхідним для заявлених цілей, із застосуванням принципів мінімізації, обмеження цілей і зберігання, а також доступом лише для уповноважених осіб і провайдерів, залучених для надання відповідних функцій .

Контроль і вибір. Для опційних функцій надаються механізми granular consent/opt-in/opt-out через налаштування облікового запису, панелі керування в продукті або посилання у комунікаціях. Відкликання згоди не впливає на законність обробки до моменту відкликання і може обмежити функціональність пов'язаних модулів або інтеграцій .

Технологічна нейтральність. Послуги можуть взаємодіяти з різними середовищами та сторонніми інтеграціями; Agent X Group LLC не визначає цілі обробки у зовнішніх середовищах і не несе відповідальності за практики третіх сторін. Для таких сервісів застосовуються їхні власні політики конфіденційності та умови, з якими слід ознайомитись окремо .

Product tiers: free, paid, custom

Дані реєстрації та ідентифікації: електронна пошта та/або номер мобільного, а також підтвердження (OTP, email verification) з метою створення акаунта, автентифікації, безпеки й комунікацій; правова підстава: виконання договору, законний інтерес у безпеці, правові зобов'язання за потреби; роль: контролер.

Дані облікового запису на сайті: пароль кабінету, нік у Telegram, реквізити гарантії для виведення реферальних винагород, які зберігаються та використовуються для налаштувань профілю, виплат і комунікацій; правова підстава: виконання договору; роль: контролер.

Збираються технічні дані: IP-адреса, тип/версія браузера, мова, дати/часи доступу, ідентифікатори пристрою, ОС, відвідані сторінки, події та журнали сервісу; мета: безпека, діагностика, протидія шахрайству, продуктивність, аналітика, відповідність вимогам; правова підстава: законний інтерес, виконання договору для працездатності, правові зобов'язання щодо безпеки; роль: контролер для власних журналів, процесор у межах функцій, що контролюються клієнтом.

Додаткові атрибути пристрою: cpu model, system UUID, baseboard model, OS serial, OS hostname, що використовуються для захисту від шахрайства, обмеження зловживань та

технічної підтримки; правова підстава: законний інтерес у безпеці та цілісності сервісу; роль: контролер.

Верифікація особи (за контекстом). Якщо цього вимагає закон, інтеграція або окремі функції, може проводитися КҮС/верифікація особи, включно з фото/біометрією, що активується окремою явною дією; мета: ідентифікація, дотримання права, безпека; правова підстава: юридичний обов'язок, істотний публічний інтерес за наявності, або згода, якщо потрібна; роль: контролер/спільні контролери/процесор залежно від моделі та провайдера.

Якщо верифікацію виконує сторонній провайдер, застосовуються його політики, а обмін даними обмежується необхідним для підтвердження статусу.

Розширена перевірка: для функцій підвищеної довіри можуть запитуватися ПІБ, ідентифікаційний номер, номер телефону та підтвердження атрибутів; відмова — обмежує доступ лише до відповідних функцій, крім випадків, коли ідентифікація є вимогою закону чи партнерського майданчика; правова підстава: виконання договору, законний інтерес, юридичний обов'язок; роль: контролер або спільні контролери/процесор залежно від інтеграції.

Дані, що обробляються: ідентифікаційні та контактні дані, довідкові документи або токени верифікації від зовнішніх провайдерів для попередження шахрайства, безпеки та виконання вимог третіх сторін; зберігання здійснюється на період, необхідний для цілей перевірки й виконання обов'язків.

Профіль та додаткові атрибути: за бажанням користувача можуть оброблятися нікнейм, фото, додаткові контакти для персоналізації, командних просторів або спільного доступу; правова підстава: згода або виконання договору для командних функцій; роль: контролер.

Операційні активності (акції/винагороди): збираються ідентифікаційні, контактні та платіжні реквізити за потреби для верифікації відповідності та виплат; відмова надавати — позбавляє права на винагороду без впливу на базові функції; правова підстава: виконання договору участі, згода для маркетингу; роль: контролер.

Хешування і унікальний ідентифікатор пристрою/акаунта

З метою запобігання шахрайству, контролю доступу та діагностики всі перелічені технічні атрибути та базові реєстраційні ідентифікатори можуть агрегуватися в нормалізований рядок, який хешується алгоритмом SHA-256; утворений хеш передається по захищеному каналу HTTPS та зберігається в базі як технічний ідентифікатор без зворотної прив'язки до первинних значень без додаткової інформації.

Такий хеш використовується для детекції аномалій, обмеження мультиакаунту, виявлення зловживань і забезпечення цілісності сесій; правова підстава: законний інтерес у безпеці та запобіганні шахрайству; збереження первинних значень здійснюється лише в тій мірі, що необхідна для технічної підтримки та безпеки, з доступом за принципом мінімальності.

Прозорість і вибір

Інформація про категорії даних, цілі, строки зберігання, підстави обробки, отримувачів і права суб'єктів надається в основних розділах Політики; для атрибутів, що потребують згоди, реалізовано механізми керування нею; доступ, виправлення, заперечення,

обмеження, переносимість та видалення реалізуються через підтримку або профіль у межах, визначених законом.

У випадку змін переліку технічних атрибутів або методів хешування Політика оновлюється із зазначенням дати набрання чинності; подальше використання сервісу означає прийняття змін, якщо інше не передбачено обов'язковими нормами.

4. Payments, quick pay and auto-renew

Обробка платежів. Для поповнення використовується виділена адреса(и) криптогаманця в мережах EVM (єдина адреса для Ethereum/Optimism/Arbitrum/Base/BNB Chain) та TRON; приймаються USDC і USDT, у TRON — лише USDT; у межах інтеграцій передаються лише мінімально необхідні дані для транзакції та AML/anti-fraud: ідентифікатори акаунта, реквізити замовлення, сума/дата, хеш(и) транзакцій, параметри безпеки пристрою/ризик-сигнали, технічні маркери платіжного методу або гаманця; правова підстава: виконання договору, юридичні обов'язки (AML/санкції), законний інтерес у запобіганні шахрайству; роль: Agent X Group LLC — контролер для власного білінгу, сторонні провайдери/блокчейн-інфраструктура — окремі контролери своїх процесів.

Стан платежів і спори. Для підтримки, бухгалтерського обліку та вирішення спорів обробляються транзакційні дані: сума/дата, валюта/мережа, адреси відправника/одержувача, хеш транзакції, статус зарахування, номер замовлення, а також контактні реквізити (ім'я/нік, email, телефон) для зворотного зв'язку; для функцій швидкої оплати й автооновлення зберігаються токени/ідентифікатори платіжних методів або прив'язки до внутрішнього балансу, що дозволяє здійснювати майбутні списання відповідно до налаштувань користувача; активація швидкої оплати/автооновлення означає надання згоди на періодичні списання згідно з правилами підписки; сторонні фінансові установи застосовують власні політики конфіденційності до даних, які вони обробляють.

Мінімізація і безпека даних. Застосовується принцип мінімізації: з платіжних подій фіксуються лише дані, потрібні для зарахування, підтвердження, бухгалтерського обліку, запобігання шахрайству, виконання податкових/санкційних зобов'язань і підтримки; передавання здійснюється через захищені канали, доступ обмежується авторизованим персоналом, строки зберігання визначаються законодавчими та договірними вимогами.

Права та вибір. Доступ, виправлення, обмеження, заперечення, переносимість і видалення реалізуються у межах, дозволених законом і технічно сумісних із вимогами бухгалтерського обліку та протидії відмиванню коштів.

5. Customer Service and Dispute Resolution

Канали і дані звернень. Під час звернень до підтримки обробляються необхідні дані для верифікації, комунікації та вирішення питання: облікові дані, контактні дані, контент звернення, записи листування/дзвінків, дані конкретного замовлення/операцій, технічні журнали, додаткові матеріали, які добровільно надані для підтвердження фактів. Мета: підтримка, безпека, якість сервісу, удосконалення продукту. Правова підстава: виконання договору; законний інтерес у забезпеченні підтримки і якості; юридичні обов'язки щодо комплаєнсу, якщо застосовно. Роль: контролер .

Опитування задоволеності. Можемо надсилати опитування або збирати фідбек щодо якості підтримки; участь добровільна, і обробка базується на згоді або законному інтересі з можливістю заперечення/відписки .

III. Providing Data to External Parties

1. Sharing

Загальний принцип. Персональні дані не передаються компаніям, організаціям чи особам поза Agent X Group LLC, окрім випадків, описаних нижче; у таких випадках одержувачі зазвичай діють як окремі контролери і застосовують власні політики конфіденційності .

Виконання правових обов'язків. Дані можуть бути надані на підставі вимог закону, запитів/наказів судів, регуляторів або для цілей судових і арбітражних проваджень, забезпечення виконання рішень чи досудового врегулювання спорів .

За вашою згодою. За наявності явної згоди дані можуть бути передані вибраним вами третім сторонам, що надають інтегровані або супутні послуги .

Виконання договору/транзакції. Для обробки замовлень, доставки, білінгу, післяпродажної підтримки та вирішення спорів необхідні транзакційні дані можуть надаватися відповідним постачальникам/провайдерам за вашим вибором (наприклад, маркетплейсам чи платіжним сервісам) .

Афілійовані особи. Для спільного надання сервісів, використання єдиного облікового запису, рекомендацій релевантних даних, виявлення аномалій акаунтів та захисту особистої і майнової безпеки користувачів/публіки дані можуть спільно використовуватись з афілійованими особами Agent X Group LLC та/або їхніми визначеними сервіс-провайдерами. Передається лише мінімально необхідний обсяг даних відповідно до цілей цієї Політики; у разі обробки чутливих даних або зміни цілей буде отримано додаткову авторизацію .

Публічне поширення користувачем. Інформація, якою користувач ділиться публічно у Послугах чи зовнішніх середовищах, може містити персональні або чутливі дані — варто зважено приймати такі рішення, оскільки контроль за такою інформацією обмежений .

Entrusted processing (Processors/Sub-processors)

Принципи. Agent X Group LLC може залучати авторизованих партнерів як процесорів/субпроцесорів для надання інфраструктури, підтримки, аналітики, платіжної обробки, досліджень і опитувань. Такі партнери отримують доступ лише до обсягу даних, необхідного для виконання доручених функцій, і зобов'язуються використовувати дані виключно в межах інструкцій та з належними заходами безпеки .

Категорії партнерів.

(a) Реклама та аналітика: обробка охоплення/ефективності за галузевими стандартами без ідентифікаторів, що прямо ідентифікують особу, якщо інше не вимагається функціоналом за окремою згодою .

(b) Постачальники інфраструктури, підтримки та платежів: хмарні провайдери, CDN, моніторинг, логування, антишахрайські сервіси, служби підтримки, платежі/білінг і дослідні організації .

Додаткова згода. Якщо процесор бажає використовувати дані поза межами наданих інструкцій або з іншою метою, він зобов'язаний отримати окрему згоду відповідного суб'єкта даних або укласти належні договірні домовленості з контролером .

Transfer (M&A/Corporate changes)

Корпоративні угоди. У разі злиття, поділу, реорганізації, продажу активів, ліквідації чи банкрутства можуть відбутися передачі даних правонаступнику. Про найменування/назву та контакти одержувача буде повідомлено; одержувач зобов'язується дотримуватися цієї Політики та застосовного права або отримати нову згоду, якщо змінюються цілі чи способи обробки .

Public Disclosure

За вашою ініціативою. Публічне розкриття можливе за активним вибором і окремою згодою користувача у конкретному контексті (наприклад, профільні каталоги, відгуки) .

Порушення та безпека. Якщо встановлено порушення закону або суттєве порушення правил платформи, або для захисту безпеки користувачів/публіки, можуть бути розкриті релевантні персональні дані (включно з характером порушення та вжитими заходами) у межах, дозволених законом і необхідних для досягнення легітимної мети .

Принципи та підходи

Захист даних є пріоритетом; застосовуються комбіновані технічні й організаційні заходи, пропорційні ризикам, з регулярним тестуванням, аудитом та журналюванням доступів за принципом мінімізації прав і Zero Trust-дефолтів.

Впроваджено захист на кількох рівнях: дані, застосунок, інфраструктура, мережа, постачальники; проводиться періодичний перегляд ефективності контролів та оновлення конфігурацій безпеки.

Технічні заходи: Ідентифікатор безпеки (SHA-256)

Для цілей антифроду, контролю доступу та діагностики визначені технічні й облікові атрибути агрегуються у нормалізований рядок за детермінованими правилами формування.

Отриманий рядок хешується алгоритмом SHA-256 із застосуванням стабільної процедури нормалізації вхідних значень; у базі зберігається лише хеш-значення та службові метадані, що не дозволяють відновити початкові атрибути без додаткової інформації.

Хеш-значення та необхідні службові маркери передаються до бекенду виключно захищеним каналом HTTPS з актуальними параметрами шифрування; між сервісами використовується TLS з перевіркою сертифікатів і, за можливості, mutual TLS.

Зберігання здійснюється у захищених середовищах із контролем доступу на основі ролей; доступ надається тільки уповноваженим особам за принципом найменших привілеїв; ведеться аудит звернень.

Хеш застосовується для виявлення аномалій, обмеження мультиакаунту, боротьби зі зловживаннями, зв'язування сесій і розслідування інцидентів; первинні значення атрибутів не передаються третім сторонам, окрім випадків, прямо передбачених законом і необхідних для безпеки або виконання юридичних обов'язків.

Періоди зберігання визначаються операційною необхідністю та законодавчими вимогами, після чого хеш-значення підлягають видаленню або архівації з подальшою деперсоналізацією.

Безпека платежів і криптоінтеграцій

Операції поповнення здійснюються через адреси в мережах EVM/TRON; зберігаються лише технічні атрибути транзакцій, необхідні для зарахування та бухгалтерського/AML обліку; приватні ключі користувачів не обробляються.

Застосовуються автоматизовані risk чекі та антифрод сигнали на рівні пристрою/сесії/мережі; підозрілі транзакції можуть бути відкладені до завершення перевірок відповідно до законних підстав обробки.

Організаційні заходи

Виділена функція ІБ, внутрішні політики, регулярні тренінги, угоди про конфіденційність, контроль доступів і ротація прав, процеси управління постачальниками і субпроцесорами з оцінкою ризиків.

Процедури управління вразливостями, змінами та інцидентами, включно з журналами аудиту, періодичними перевірками доступів і принципом need to know.

План реагування на інциденти

Діє план IR: виявлення, стримування, усунення, відновлення, пост аналіз; визначено RACI, канали ескалації, взаємодію з провайдерами/партнерами, управління вразливостями та реагування на шкідливе ПЗ, мережеві атаки й спроби несанкціонованого доступу.

Проводяться навчальні тренування (table top/blue team), ретроспективи та оновлення політик за результатами інцидентів.

Повідомлення про інциденти

У разі інциденту з персональними даними повідомлення надсилається в розумні строки через доступні канали з описом характеру події, можливих наслідків і вжитих заходів; за неможливості індивідуального інформування публікується загальне повідомлення; повідомлення регуляторам — у межах вимог застосовного права.

За потреби здійснюється взаємодія з правоохоронними та наглядовими органами, а також користувачам надаються рекомендації зі зниження ризиків.

Спільна відповідальність за безпеку

Рекомендується використовувати сильні паролі, увімкнути MFA, підтримувати оновлення клієнтів, керувати сесіями та дозволами, створювати резервні копії критичних даних і перевіряти налаштування безпеки робочих просторів.

Поради з кібергігієни та актуальні рекомендації публікуються у довідкових матеріалах сервісу.

Обмеження та форс мажор. Повна безпека не може бути гарантована через технологічні обмеження і зовнішні фактори, включно з інцидентами у третіх сторін; у випадку масштабних кібератак, збоїв хмарних провайдерів, інцидентів у ланцюгу постачання чи санкційних обмежень вживаються комерційно розумні заходи для мінімізації наслідків і відновлення роботи згідно з форс мажорними положеннями Умов користування .

V. Your rights

Огляд. Залежно від застосовного права (наприклад, GDPR/EEA, UK, Швейцарія та ін.), суб'єктам даних можуть належати права доступу, виправлення, видалення, обмеження, заперечення, портативності, відкликання згоди, а також право не підлягати рішенням, що ґрунтуються виключно на автоматизованій обробці, якщо такі рішення мають правові наслідки або подібним чином істотно впливають. Нижче наведено механізми реалізації цих прав через налаштування акаунта та канали підтримки .

Доступ і виправлення. Дані акаунта можна переглядати і виправляти у «Settings → My Account». Також запити приймаються через службу підтримки або email, указаний у Політиці/Умовах; можуть знадобитися верифікаційні кроки для захисту облікового запису

Видалення даних. Можна видаляти окремі дані через «Settings → My Account» або ініціювати видалення акаунта. У випадках, передбачених законом або Політикою (відкликання згоди; припинення цілей; закінчення строків зберігання; припинення надання послуг), можна подати запит на видалення через службу підтримки .

Резервні копії. Видалення означає усунення даних із систем, що забезпечують повсякденну роботу. Через технічні та правові обмеження миттєве видалення з резервних копій може бути неможливим; у такому разі дані зберігаються без активної обробки і будуть безпечно очищені чи анонімізовані за розкладом ротації бекапів .

Сповіщення одержувачів. У разі видалення Agent X Group LLC докладе комерційно розумних зусиль, щоб повідомити одержувачів, яким дані були розкриті, про необхідність видалення, якщо це не суперечить закону або якщо одержувач не має незалежних правових підстав для подальшої обробки .

Керування згодами. Обсяг наданих згод можна змінити у «My → Account and Security» або через службу підтримки. Відкликання згоди діє на майбутнє і не впливає на законність обробки, здійсненої до відкликання. Для даних, необхідних для базових функцій або виконання юридичних обов'язків, зміна згоди може бути недоступною .

Скасування акаунта. Запит подається через підтримку або у клієнті: «Account Settings → Account Cancellation». Після верифікації особи/безпеки/пристрою надання Послуг припиняється, а персональні дані видаляються або анонімізуються відповідно до права та внутрішньої політики зберігання. Дія є незворотною; дані не підлягають відновленню, якщо інше не вимагається законом або стандартами .

Додаткові умови. Перед поданням заявки варто ознайомитися з чинною угодою про видалення/деактивацію. Повторне використання Послуг після скасування потребує нової реєстрації згідно з правилами платформи .

Автоматизовані рішення. Якщо певні рішення ґрунтуються виключно на автоматизованій обробці (включно з алгоритмами) і мають правові наслідки або істотно впливають, можна звернутися до підтримки для отримання пояснень, оскарження або втручання людини, якщо це вимагається застосовним правом .

Подання запитів. Запити можуть подаватися особисто суб'єктом даних або, де це передбачено правом, законними представниками (опікунами, близькими родичами після смерті, тощо). Для захисту облікового запису може знадобитися верифікація особи (додаткова перевірка акаунта, письмовий запит тощо) .

Строки і плата. Відповідь на обґрунтовані запити надається у розумний строк, як правило,

Для запобігання несанкціонованому доступу проводяться розумні кроки верифікації (додаткова авторизація акаунта, письмовий запит, підтверджуючі відомості).

Відповідь надається у розумний строк, як правило, до 15 днів або в строк, передбачений застосовним правом (наприклад, до 30/45 днів із можливим продовженням за складності запиту).

Обґрунтовані запити безкоштовні; надмірні/повторювані можуть бути платними.

Запити можуть бути відхилені, якщо вони: необґрунтовано повторні; технічно непропорційні (вимагають створення нових систем чи фундаментальної зміни практик); порушують права інших; суперечать закону або законним інтересам у сфері безпеки, протидії шахрайству чи збереження доказів. У таких випадках надається мотивоване пояснення, якщо не заборонено законом.

Резервні копії, журнали і затримки видалення

Дані в резервних копіях зберігаються ізоляційно й без активної обробки до завершення циклу ротації/очищення; коли технічно можливе вибіркове очищення — застосовується; інакше використовується політика «no restore unless required by law/incident».

Журнали та телеметрія. Окремі журнали безпеки/доступів/платежів можуть зберігатися довше для цілей аудиту, комплаєнсу, безпеки та розслідувань, відповідно до правових вимог і принципу мінімізації.

Регіональні зауваги (приклади)

ЄЄЗ/Велика Британія/Швейцарія. Права встановлюються GDPR/UK GDPR та національним правом; існує право подати скаргу до наглядового органу (наприклад, DPA/ICO). Міжнародні передачі захищаються відповідними механізмами (наприклад, стандартні договірні положення).

Інші юрисдикції. Додаткові або відмінні права можуть надаватися місцевим правом; у таких випадках у Політиці можуть бути окремі розділи або додатки.

VI. Storage of data

Принцип строків зберігання. Персональні дані зберігаються лише стільки, скільки необхідно для досягнення цілей, описаних у цій Політиці, виконання договору, дотримання юридичних обов'язків і забезпечення безпеки/цілісності Послуг, за винятком випадків, коли застосовне право встановлює інші мінімальні або конкретні строки зберігання.

Критерії визначення строків. Під час визначення періоду зберігання враховуються, зокрема:

1. завершення операцій/транзакцій, ведення відповідних бізнес-записів, обробка претензій, повернень, chargeback і вирішення спорів;
2. забезпечення безпеки, якості, аудиту, журналювання доступів і розслідувань інцидентів;
3. наявність наданої згоди на довший строк (де це дозволено і до моменту відкликання);

4. спеціальні договори або конкретні правові вимоги щодо зберігання (наприклад, бухгалтерські/податкові норми, AML/санкційні перевірки, строки позовної давності) .

Приклади категорій і типові строки.

5. Облікові дані: протягом дії акаунта та розумного періоду після деактивації для закриття операцій, виконання вимог права та вирішення спорів .
6. Журнали безпеки/доступів: зберігаються стільки, скільки потрібно для забезпечення безпеки, аудиту та комплаєнсу відповідно до внутрішньої політики і закону .
7. Платіжні та білінгові записи: відповідно до бухгалтерських і податкових вимог, а також строків позовної давності, передбачених правом .

Застосовне право і *lex specialis*. Якщо закон встановлює конкретні мінімальні строки (наприклад, вимоги електронної комерції щодо збереження даних про товари/послуги і транзакції не менше визначеного періоду), такі строки мають пріоритет перед загальними правилами цієї Політики .

Резервні копії і відновлення. Дані в резервних копіях зберігаються ізоляційно, без активної обробки, виключно для цілей відновлення після інцидентів або на вимогу закону. Після завершення циклу ротації бекапи безпечно очищуються або анонімізуються; вибіркоче очищення застосовується там, де це технічно здійснено .

Міжнародні зберігання/передачі. При залученні хмарних або інфраструктурних провайдерів дані можуть оброблятися у різних юрисдикціях із застосуванням належних механізмів міжнародних передач і договірних гарантій субпроцесингу, з дотриманням принципів мінімізації та обмеження доступу .

Безпечне видалення/анонімізація. Після закінчення строків зберігання персональні дані видаляються або анонімізуються із застосуванням комерційно розумних технічних і організаційних процедур, які запобігають несанкціонованому доступу, відтворенню або деанонімізації. Для носіїв використовується безпечна утилізація відповідно до галузевих стандартів .

Захист під час зберігання. На період зберігання застосовуються пропорційні заходи безпеки: шифрування при передачі і, де доречно, при зберіганні; контроль доступу (RBAC/MFA); мережеві бар'єри; моніторинг і журналювання; регулярні перевірки доступів і тестування планів відновлення .

VII. Policy Updates

- Принцип оновлень. Ця Політика може періодично оновлюватися для відображення змін у продуктах, сервісах, технологіях або правових вимогах. Якщо інше не вимагається застосовним правом, оновлена редакція набирає чинності з моменту її публікації у Послугах; подальший доступ або використання Послуг означає згоду з оновленою Політикою. Якщо положення є неприйнятними, використання слід припинити до набрання чинності змінами .
- Відсутність звуження прав без згоди. Без явної згоди суб'єктів даних Agent X Group LLC не буде звужувати права, прямо надані цією Політикою, у межах, де таку згоду

вимагає застосовне право. У випадках, коли закон дозволяє односторонні зміни без отримання згоди, зміни можуть бути внесені шляхом публікації .

Суттєві зміни. До «суттєвих» належать, зокрема:

- зміни у категоріях даних, що збираються, або в цілях/правових підставах обробки;
- нові типи одержувачів/міжнародних передач;
- значні зміни у строках зберігання або правах суб'єктів;
- зміни у відповідальних суб'єктах (наприклад, афілійовані компанії/ правонаступники) .

Повідомлення. Про суттєві зміни може бути повідомлено більш помітно, зокрема через публічне повідомлення на сайті, вбудовані банери/поп-апи, in-app повідомлення або email/SMS за наявності контактів. Спосіб повідомлення обирається на розсуд Agent X Group LLC з урахуванням характеру змін і практичної досяжності каналів .

Дата набрання чинності. У верхній частині Політики зазначається дата останнього оновлення; окремі зміни можуть мати відстрочену дату набрання чинності, якщо це необхідно для технічної імплементації або виконання вимог права .

VIII. Protection of Minors

Загальні положення. Послуги Agent X Group LLC призначені для повнолітніх користувачів. Якщо застосовне право визначає особу як неповнолітню, використання Послуг і надання персональних даних дозволяються лише за згодою та під наглядом батьків або законних опікунів, після уважного ознайомлення з цією Політикою та політиками сторонніх додатків/інтеграцій, де це релевантно .

Обробка даних дітей. Персональні дані неповнолітніх обробляються лише за наявності правової підстави: дозволу закону, явної та верифікованої згоди батьків/опікунів, або якщо обробка необхідна для захисту життєво важливих інтересів дитини. Обсяг даних обмежується необхідним мінімумом для заявленої мети, із застосуванням підвищених заходів безпеки .

Верифікація і видалення. Якщо буде виявлено, що дані неповнолітнього були зібрані без перевіреної батьківської згоди, Agent X Group LLC вживе заходів для своєчасного видалення або анонімізації таких даних. Батьки/опікуни можуть звернутися через канали, наведені в розділі «Contact Us», для запитів щодо доступу, виправлення або видалення даних неповнолітнього .

IX. Contact Us

Канали звернень. Питання, коментарі чи пропозиції щодо цієї Політики, а також запити на реалізацію прав суб'єктів даних приймаються через:

- онлайн-підтримку в Послугах;
- email: office@agentx.company;
- інші доступні канали, зазначені у відповідних інтерфейсах (in-app, веб-форма). Запити, не пов'язані з цією Політикою або правами у сфері персональних даних, можуть не розглядатися через ці канали .

Процедура опрацювання. Для захисту облікового запису може знадобитися верифікація особи. Відповіді надаються у розумний строк, як правило, протягом 15–30 днів або відповідно до вимог застосовного права. Якщо питання стосується інтеграцій третіх сторін, може знадобитися звернення до цих третіх сторін згідно з їхніми політиками .