Privacy Policy

Introduction

Welcome to Agent X Group LLC products and services. This Privacy Policy ("Policy") explains how personal data is processed when accessing and using websites, applications, clients, APIs, integrations, plugins, SDKs, and other technological interfaces and form factors (collectively, the "Services"). The Services are technology-neutral tools and do not determine the purposes for which users use them in external environments.

Please read this Policy carefully before using the Services. Continued access or use, as well as actions such as "agree," registration, download, installation, or login, mean that the Policy has been read and accepted, including consent to the processing of the necessary categories of personal data to provide basic and additional features, as described below. If the provisions are unacceptable, you should discontinue use of the Services.

Contractual Integration. This Policy is an integral part of the Agent X Group LLC Terms of Use. In the event of any conflict between these documents, the provisions that ensure the provision of the Services in compliance with data protection requirements shall apply; the disclaimer of warranties and limitation of liability provisions in the Terms of Use shall apply to this Policy to the maximum extent permitted by law.

Roles under the GDPR. Depending on the processing function:

- Controller: Agent X Group LLC acts as a controller where it independently determines the purposes and means of processing (e.g., billing, security, account management, analytics, communications).
- Processor: Agent X Group LLC acts as a processor when it processes data on behalf of a customer for functions that the customer initiates and controls (e.g., profile synchronization, team access, workspaces, integrations). In these cases, the customer is the controller and is responsible for the legal basis, appropriate notifications to data subjects, and the exercise of their rights.

Consent and other legal bases. Where consent is required, it is provided in an explicit manner through interfaces or account settings and can be withdrawn at any time with future effect through the appropriate mechanisms. In other cases, processing may be based on the performance of a contract, legitimate interest, legal obligations, or the protection of vital interests, depending on the context, as detailed in the individual sections of the Policy.

Policy Updates. The Policy may be changed from time to time by posting an updated version on the Services without prior notice. Continued use after changes are posted constitutes acceptance of the updated Policy; if you do not agree, you may limit processing or discontinue use of the Services through settings or account deletion.

Geographic Scope. This Policy applies to data processing regardless of the user's location; for residents of the EEA/UK/Switzerland, California, and other jurisdictions with specific requirements, specific sections contain additional information about the rights and requirements of local law.

Contact Channels. Questions regarding this Policy or the exercise of data subjects' rights may be sent to officce@agentx.company or through the designated support channels in the Services. Channels may change over time in a technology-neutral manner.

I. Scope

Scope of the Policy. This Policy applies to the processing of personal data in connection with the use of Agent X Group LLC products and services provided through websites, software clients, mobile applications, weband desktop interfaces, APIs, integrations, plugins, SDKs, and other current or future technology channels and form factors that may emerge as a result of technological developments (collectively, the "Services").

Technology Neutrality. The Services are technology-neutral tools; the determination of the purposes and means of use in external environments (e.g., on third-party platforms) is not controlled by Agent X Group LLC, and responsibility for such use lies with the user or the relevant data controller, depending on the context.

Exceptions. This Policy does not apply to products/services of partners or other third parties, even if they are integrated or accessible through the Services (e.g., third-party extensions, marketplaces, payment providers, cloud services). Such services are governed by their own privacy policies and terms, which should be reviewed separately.

Roles of the parties. When Agent X Group LLC processes data on behalf of a customer within the scope of functions initiated/controlled by the customer, Agent X Group LLC acts as a processor and the customer acts as a controller. If Agent X Group LLC independently determines the purposes and means of processing (e.g., billing, security, analytics), it acts as a controller; in this case, this Policy should be read in conjunction with the Terms of Use and relevant policies of Agent X Group LLC.

Territorial scope. The Policy applies to data processing regardless of the user's location; additional notices may apply to residents of the EEA/UK/Switzerland, California, and other jurisdictions with specific requirements.

II. Data Collection and Use

General Principles. When using the Services, personal data may be collected and processed to provide basic and additional features. The categories of data, purposes, legal grounds, retention periods, and control settings depend on the selected modules, integrations, and pricing plan, as well as on the role of Agent X Group LLC as a controller or processor in a specific context.

Basic functions (required data). Certain data is required to launch an account, for authentication, billing, security, support, customer enablement, synchronization of critical environment settings, and contract fulfillment. Refusal to provide such data may make it impossible to access or use the basic functions of the Services.

Additional features (optional data). Certain advanced features—such as team access and shared workspaces, third-party integrations, analytics dashboards, consent-based marketing communications, performance improvement telemetry, and beta features—may require additional data. Consent to such processing is voluntary and can be provided/withdrawn through settings; refusal does not affect access to basic features, but may limit or change the operation of the relevant additional modules.

Module variability. Since the set of functional modules and integrations varies between users, specific data categories and the scope of processing may differ. Detailed descriptions are

available in the relevant module interfaces and reference materials in the Services; when a specific function is activated, relevant information about data categories, purposes, legal grounds, and control settings is displayed.

Legal bases. Core data processing is primarily performed to fulfill a contract, comply with legal obligations, and ensure the security/integrity of the service; for optional processing, consent or legitimate interest may be used, with a balancing test and opt-out mechanisms provided where applicable. For scenarios where Agent X Group LLC acts as a processor, the legal basis is determined by the controller (client) and provides appropriate notifications to data subjects.

Minimization and proportionality. Data collection and use are limited to what is necessary for the stated purposes, applying the principles of minimization, purpose limitation, and storage limitation, as well as access only by authorized persons and providers involved in providing the relevant functions.

Control and choice. For optional features, granular consent/opt-in/opt-out mechanisms are provided through account settings, product control panels, or links in communications. Withdrawal of consent does not affect the lawfulness of processing prior to withdrawal and may limit the functionality of related modules or integrations.

Technology neutrality. Services may interact with various environments and third-party integrations; Agent X Group LLC does not determine the purposes of processing in external environments and is not responsible for the practices of third parties. Such services are subject to their own privacy policies and terms and conditions, which should be reviewed separately.

Product tiers: free, paid, custom

Registration and identification data: email and/or mobile number, as well as confirmation (OTP, email verification) for the purpose of account creation, authentication, security, and communications; legal basis: performance of a contract, legitimate interest in security, legal obligations as necessary; role: controller.

Website account data: account password, Telegram nickname, wallet details for withdrawing referral rewards, which are stored and used for profile settings, payments, and communications; legal basis: performance of a contract; role: controller.

Technical data collected: IP address, browser type/version, language, access dates/times, device identifiers, OS, pages visited, events, and service logs; purpose: security, diagnostics, fraud prevention, performance, analytics, compliance; legal basis: legitimate interest, performance of a contract for operability, legal security obligations; role: controller for own logs, processor within the scope of functions controlled by the client.

Additional device attributes: CPU model, system UUID, baseboard model, OS serial, OS hostname, used for fraud protection, abuse prevention, and technical support ; legal basis: legitimate interest in security and integrity of the service; role: controller.

Identity verification (contextual). If required by law, integration, or specific features, KYC/identity verification may be performed, including photo/biometrics, activated by a separate explicit action; purpose: identification, legal compliance, security; legal basis: legal obligation, substantial public interest where applicable, or consent where required; role: controller/joint controllers/processor depending on the model and provider.

If verification is performed by a third-party provider, its policies apply, and data sharing is limited to what is necessary to confirm status.

Enhanced verification: for high-trust features, full name, identification number, phone number, and attribute confirmation may be requested; refusal — restricts access only to the relevant features, except where identification is required by law or a partner platform; legal basis: performance of a contract, legitimate interest, legal obligation; Role: controller or joint controllers/processor depending on integration.

Data processed: identification and contact details, reference documents or verification tokens from external providers for fraud prevention, security, and compliance with third-party requirements; storage is carried out for the period necessary for verification and performance of duties.

Profile and additional attributes: at the user's request, nicknames, photos, additional contacts for personalization, team spaces, or shared access may be processed; legal basis: consent or performance of a contract for team functions; role: controller.

Operational activities (actions/rewards): identification, contact, and payment details are collected as needed for verification of compliance and payments; refusal to provide this information results in forfeiture of the right to rewards without affecting basic functions; legal basis: performance of a participation agreement, consent for marketing; role: controller.

Hashing and unique device/account identifier

For the purposes of fraud prevention, access control, and diagnostics, all of the above technical attributes and basic registration identifiers may be aggregated into a normalized string that is hashed using the SHA-256 algorithm; The resulting hash is transmitted over a secure HTTPS channel and stored in the database as a technical identifier without a reverse link to the original values and without additional information.

This hash is used to detect anomalies, limit multi-accounting, identify abuse, and ensure session integrity. Legal basis: legitimate interest in security and fraud prevention. The original values are retained only to the extent necessary for technical support and security, with access based on the principle of minimality.

Transparency and choice

Information about data categories, purposes, storage periods, grounds for processing, recipients, and the rights of data subjects is provided in the main sections of the Policy; for attributes requiring consent, control mechanisms are implemented; access, correction, objection, restriction, portability, and deletion are implemented through support or profile within the limits defined by law.

In the event of changes to the list of technical attributes or hashing methods, the Policy is updated with the date of entry into force; continued use of the service implies acceptance of the changes, unless otherwise provided by mandatory regulations.

4. Payments, quick pay, and auto-renew

Payment processing. Topping up is done using a dedicated crypto wallet address(es) on the EVM (single address for Ethereum/Optimism/Arbitrum/Base/BNB Chain) and TRON networks; USDC and USDT are accepted, in TRON — only USDT; only the minimum data necessary for the transaction and AML/anti-fraud is transferred within the integrations: account identifiers, order details, amount/date, transaction hash(es), device security parameters/risk signals, technical markers of the payment method or wallet; Legal basis: performance of a contract, legal obligations (AML/sanctions), legitimate interest in fraud prevention. Role: Agent X Group LLC

is the controller for its own billing, third-party providers/blockchain infrastructure are separate controllers of their own processes.

Payment status and disputes. Transaction data is processed for support, accounting, and dispute resolution: amount/date, currency/network, sender/recipient addresses, transaction hash, credit status, order number, and contact details (name/nickname, email, phone number) for feedback; For quick payment and auto-renewal features, payment method tokens/identifiers or links to internal balances are stored, allowing future debits to be made according to user settings; activation of quick payment/auto-renewal means consent to periodic debits in accordance with the subscription rules. Third-party financial institutions apply their own privacy policies to the data they process.

Data minimization and security. The principle of minimization is applied: only data necessary for crediting, confirmation, accounting, fraud prevention, tax/sanctions compliance, and support is recorded from payment events. transfers are made through secure channels, access is restricted to authorized personnel, and retention periods are determined by legal and contractual requirements.

Rights and choices. Access, correction, restriction, objection, portability, and deletion are implemented to the extent permitted by law and technically compatible with accounting and antimoney laundering requirements.

5. Customer Service and Dispute Resolution

Channels and data of requests. When contacting support, the necessary data for verification, communication, and resolution of the issue is processed: account details, contact details, content of the request, correspondence/call records, specific order/transaction data, technical logs, additional materials voluntarily provided to confirm the facts. Purpose: support, security, service quality, product improvement. Legal basis: performance of a contract; legitimate interest in ensuring support and quality; legal compliance obligations, if applicable. Role: controller.

Satisfaction surveys. We may send surveys or collect feedback on the quality of support; participation is voluntary, and processing is based on consent or legitimate interest with the possibility of objection/unsubscription. III. Providing Data to External Parties

1. Sharing

General Principle. Personal data is not transferred to companies, organizations, or individuals outside of Agent X Group LLC, except in the cases described below; in such cases, the recipients typically act as separate controllers and apply their own privacy policies.

Compliance with Legal Obligations. Data may be provided based on legal requirements, requests/orders from courts, regulators, or for the purposes of court and arbitration proceedings, enforcement of decisions, or pre-trial settlement of disputes.

With your consent. With your explicit consent, data may be transferred to third parties selected by you that provide integrated or related services.

Performance of a contract/transaction. Transaction data necessary for order processing, delivery, billing, after-sales support, and dispute resolution may be provided to relevant suppliers/providers of your choice (e.g., marketplaces or payment services).

Affiliates. For the joint provision of services, use of a single account, recommendations of relevant data, detection of account anomalies, and protection of the personal and property

security of users/the public, data may be shared with affiliates of Agent X Group LLC and/or their designated service providers. Only the minimum amount of data necessary for the purposes of this Policy will be transferred; in the event of sensitive data processing or a change in purpose, additional authorization will be obtained.

Public disclosure by the user. Information that the user shares publicly in the Services or external environments may contain personal or sensitive data — such decisions should be made carefully, as control over such information is limited.

Entrusted processing (Processors/Sub-processors)

Principles. Agent X Group LLC may engage authorized partners as processors/sub-processors to provide infrastructure, support, analytics, payment processing, research, and surveys. Such partners only get access to the amount of data needed to do their jobs and agree to only use the data as instructed and with the right security measures.

Categories of Partners.
(a) Advertising and analytics: processing of reach/performance by industry standards without identifiers that directly identify an individual, unless otherwise required by functionality under a separate agreement.
(b) Infrastructure, support, and payment providers: cloud providers, CDNs, monitoring, logging, anti-fraud services, support services, payments/billing, and research organizations.

Additional consent. If the processor wishes to use the data outside the scope of the instructions provided or for another purpose, it must obtain separate consent from the relevant data subject or enter into appropriate contractual arrangements with the controller.

Transfer (M&A/Corporate changes)

Corporate transactions. In the event of a merger, division, reorganization, sale of assets, liquidation, or bankruptcy, data may be transferred to a successor. The name and contact details of the recipient will be disclosed; the recipient undertakes to comply with this Policy and applicable law or to obtain new consent if the purposes or methods of processing change.

Public Disclosure

At your initiative. Public disclosure is possible with the active choice and separate consent of the user in a specific context (e.g., profile directories, reviews).

Violations and security. If a violation of the law or a material violation of the platform rules is established, or to protect the safety of users/the public, relevant personal data (including the nature of the violation and the measures taken) may be disclosed to the extent permitted by law and necessary to achieve a legitimate purpose.

Principles and approaches

Data protection is a priority; combined technical and organizational measures are applied, proportionate to the risks, with regular testing, auditing, and logging of access based on the principle of minimizing rights and Zero Trust defaults.

Multi-level protection is implemented: data, application, infrastructure, network, suppliers; periodic review of control effectiveness and security configuration updates are performed.

Technical measures: Security identifier (SHA-256)

For anti-fraud, access control, and diagnostic purposes, specified technical and accounting attributes are aggregated into a normalized string according to deterministic formation rules.

The resulting string is hashed using the SHA-256 algorithm with a stable input normalization procedure; only the hash value and service metadata are stored in the database, which does not allow the original attributes to be recovered without additional information.

The hash value and necessary service markers are transmitted to the backend exclusively via a secure HTTPS channel with up-to-date encryption parameters; TLS with certificate verification and, where possible, mutual TLS is used between services.

Storage is carried out in secure environments with role-based access control; access is granted only to authorized persons according to the principle of least privilege; requests are audited.

Hashes are used to detect anomalies, limit multi-accounting, combat abuse, link sessions, and investigate incidents; the original attribute values are not transferred to third parties, except in cases expressly provided for by law and necessary for security or the fulfillment of legal obligations.

Retention periods are determined by operational necessity and legal requirements, after which hash values are subject to deletion or archiving with subsequent depersonalization.

Payment and crypto integration security

Deposit transactions are carried out via addresses in the EVM/TRON networks; only the technical attributes of transactions necessary for crediting and accounting/AML records are stored; users' private keys are not processed.

Automated risk checks and anti-fraud signals are applied at the device/session/network level; suspicious transactions may be postponed until checks are completed in accordance with the legal grounds for processing.

Organizational measures

Dedicated IT security function, internal policies, regular training, confidentiality agreements, access control and rotation of rights, supplier and subcontractor management processes with risk assessment.

Vulnerability, change, and incident management procedures, including audit logs, periodic access reviews, and the need-to-know principle.

Incident response plan

IR plan in place: detection, containment, elimination, recovery, post-analysis; RACI, escalation channels, interaction with providers/partners, vulnerability management and response to malicious software, network attacks and unauthorized access attempts defined.

Training exercises (table top/blue team), retrospectives, and policy updates are conducted based on incident results. Incident reporting

In the event of a personal data incident, a notification is sent within a reasonable time through available channels, describing the nature of the incident, possible consequences, and measures

taken; if individual notification is not possible, a general notification is published; notifications to regulators are made in accordance with applicable law.

If necessary, law enforcement and supervisory authorities are notified, and users are provided with recommendations to mitigate risks.

Shared responsibility for security

It is recommended to use strong passwords, enable MFA, keep clients up to date, manage sessions and permissions, back up critical data, and check the security settings of workspaces.

Cyber hygiene tips and current recommendations are published in the service's reference materials.

Limitations and force majeure. Complete security cannot be guaranteed due to technological limitations and external factors, including third-party incidents. In the event of large-scale cyberattacks, cloud provider failures, supply chain incidents, or sanctions restrictions, commercially reasonable measures will be taken to minimize the impact and restore operations in accordance with the force majeure provisions of the Terms of Use.

V. Your rights

Overview. Depending on the applicable law (e.g., GDPR/EEA, UK, Switzerland, etc.), data subjects may have rights of access, rectification, erasure, restriction, objection, portability, withdrawal of consent, and the right not to be subject to decisions based solely on automated processing, if such decisions have legal effects or similarly significantly affect them. Below are the mechanisms for exercising these rights through account settings and support channels.

Access and correction. Account data can be viewed and corrected in "Settings → My Account." Requests are also accepted through customer support or the email address specified in the Policy/Terms; verification steps may be required to protect your account.

Data deletion. You can delete individual data via "Settings → My Account" or initiate account deletion. In cases provided for by law or the Policy (withdrawal of consent; termination of purposes; expiration of storage periods; termination of services), you can submit a deletion request via support.

Backups. Deletion means removing data from systems that support day-to-day operations. Due to technical and legal constraints, immediate deletion from backups may not be possible; in such cases, data is stored without active processing and will be securely erased or anonymized according to the backup rotation schedule.

Notification of recipients. In the event of deletion, Agent X Group LLC will use commercially reasonable efforts to notify recipients to whom the data has been disclosed of the need for deletion, unless this is contrary to the law or unless the recipient has independent legal grounds for further processing.

Managing consents. The scope of consents given can be changed in "My → Account and Security" or through customer support. Withdrawal of consent is effective for the future and does not affect the lawfulness of processing carried out prior to withdrawal. For data necessary for basic functions or to fulfill legal obligations, changing consent may not be available.

Account cancellation. The request is submitted via support or in the client: "Account Settings → Account Cancellation." After verification of identity/security/device, the provision of Services is terminated and personal data is deleted or anonymized in accordance with the law and internal

storage policy. This action is irreversible; data cannot be recovered unless otherwise required by law or standards.

Additional conditions. Before submitting a request, please review the current deletion/deactivation agreement. Reuse of the Services after cancellation requires re-registration in accordance with the platform rules.

Automated decisions. If certain decisions are based solely on automated processing (including algorithms) and have legal consequences or significantly affect you, you may contact support for an explanation, appeal, or human intervention if required by applicable law.

Submitting requests. Requests may be submitted in person by the data subject or, where provided by law, by legal representatives (guardians, close relatives after death, etc.). Identity verification (additional account verification, written request, etc.) may be required to protect your account.

Timeframes and fees. Responses to valid requests are provided within a reasonable timeframe, typically

Reasonable verification steps (additional account authorization, written request, supporting information) are taken to prevent unauthorized access.

Responses are provided within a reasonable time, typically within 15 days or within the time frame required by applicable law (e.g., up to 30/45 days, with possible extensions for complex requests).

Reasonable requests are free of charge; excessive/repeated requests may be subject to a fee.

Requests may be denied if they are: unreasonably repetitive; technically disproportionate (requiring the creation of new systems or fundamental changes in practices); infringing on the rights of others; contrary to law or legitimate interests in the areas of security, fraud prevention, or evidence preservation. In such cases, a reasoned explanation will be provided, unless prohibited by law.

Backups, logs, and deletion delays

Data in backups is stored in isolation and without active processing until the rotation/purge cycle is complete; when selective purging is technically possible, it is applied; otherwise, a "no restore unless required by law/incident" policy is used.

Logs and telemetry. Individual security/access/payment logs may be stored longer for audit, compliance, security, and investigation purposes, in accordance with legal requirements and the principle of minimization.

Regional considerations (examples)

EEA/UK/Switzerland. Rights are established by GDPR/UK GDPR and national law; there is a right to lodge a complaint with a supervisory authority (e.g., DPA/ICO). International transfers are protected by appropriate mechanisms (e.g., standard contractual clauses).

Other jurisdictions. Additional or different rights may be granted by local law; in such cases, there may be separate sections or appendices in the Policy.

VI. Storage of data

Principle of storage periods. Personal data is stored only for as long as necessary to achieve the purposes described in this Policy, perform a contract, comply with legal obligations, and ensure

the security/integrity of the Services, unless applicable law establishes other minimum or specific storage periods.

Criteria for determining retention periods. When determining the retention period, the following factors are taken into account, among others:

1. completion of operations/transactions, maintenance of relevant business records, processing of claims, returns, chargebacks, and dispute resolution;
2. ensuring security, quality, auditing, access logging, and incident investigation;
3. the existence of consent for a longer period (where permitted and until revoked);
4. special agreements or specific legal requirements for storage (e.g., accounting/tax regulations, AML/sanctions checks, statute of limitations).

Examples of categories and typical retention periods.

- Account data: for the duration of the account and a reasonable period after deactivation to close transactions, comply with legal requirements, and resolve disputes.
- Security/access logs: retained as long as necessary to ensure security, audit, and compliance in accordance with internal policies and law.
- Payment and billing records: in accordance with accounting and tax requirements, as well as the statute of limitations provided for by law.

Applicable law and lex specialis. If the law establishes specific minimum periods (for example, e-commerce requirements to retain data on goods/services and transactions for at least a specified period), such periods shall take precedence over the general rules of this Policy.

Backups and recovery. Data in backups is stored in isolation, without active processing, solely for the purposes of recovery from incidents or as required by law. After the rotation cycle is complete, backups are securely erased or anonymized; selective erasure is applied where technically feasible.

International storage/transfer. When using cloud or infrastructure providers, data may be processed in different jurisdictions using appropriate international transfer mechanisms and contractual subprocessing safeguards, in accordance with the principles of minimization and access restriction.

Secure deletion/anonymization. At the end of the retention period, personal data is deleted or anonymized using commercially reasonable technical and organizational procedures that prevent unauthorized access, reproduction, or de-anonymization. Media is securely disposed of in accordance with industry standards.

Protection during storage. Proportionate security measures are applied during the storage period: encryption during transmission and, where appropriate, during storage; access control (RBAC/MFA); network barriers; monitoring and logging; regular access checks and testing of recovery plans.

VII. Policy Updates

- Updates Policy. This Policy may be updated periodically to reflect changes in products, services, technologies, or legal requirements. Unless otherwise required by applicable law, the updated version will take effect upon its publication in the Services; continued access or use of the Services constitutes acceptance of the updated Policy. If any provision is unacceptable, use should be discontinued prior to the changes taking effect.
- No Narrowing of Rights Without Consent. Without the express consent of data subjects, Agent X Group LLC will not narrow the rights expressly granted by this Policy to the extent that such consent is required by applicable law. In cases where the law permits unilateral changes without consent, changes may be made by posting them.

Material changes. "Material" includes, but is not limited to:

- changes in the categories of data collected or in the purposes/legal grounds for processing;
- new types of recipients/international transfers;
- significant changes in retention periods or rights of data subjects;
- changes in responsible entities (e.g., affiliated companies/successors).

Notification. Material changes may be communicated more prominently, including through a public notice on the website, embedded banners/pop-ups, in-app notifications, or email/SMS if contacts are available. The method of notification is at the discretion of Agent X Group LLC, taking into account the nature of the changes and the practical reach of the channels.

Effective date. The date of the last update is indicated at the top of the Policy; certain changes may have a delayed effective date if necessary for technical implementation or compliance with legal requirements.

VIII. Protection of Minors

General Provisions. Agent X Group LLC's Services are intended for adult users. If applicable law defines a person as a minor, the use of the Services and the provision of personal data are permitted only with the consent and supervision of parents or legal guardians, after careful review of this Policy and the policies of third-party applications/integrations, where relevant.

Processing of Children's Data. Personal data of minors is processed only if there is a legal basis: permission by law, explicit and verified consent of parents/guardians, or if processing is necessary to protect the vital interests of the child. The amount of data is limited to the minimum necessary for the stated purpose, with enhanced security measures in place.

Verification and deletion. If it is discovered that a minor's data has been collected without verified parental consent, Agent X Group LLC will take steps to promptly delete or anonymize such data. Parents/guardians may contact us through the channels listed in the "Contact Us" section for requests to access, correct, or delete a minor's data.

IX. Contact Us

Contact Channels. Questions, comments, or suggestions regarding this Policy, as well as requests to exercise data subject rights, are accepted through:

- online support in Services;

- email: office@agentx.company;
- other available channels specified in the relevant interfaces (in-app, web form). Requests not related to this Policy or personal data rights may not be considered through these channels.

Processing procedure. Identity verification may be required to protect your account. Responses are provided within a reasonable time, typically within 15-30 days or in accordance with applicable law. If the issue concerns third-party integrations, it may be necessary to contact those third parties in accordance with their policies.