X2PROXY

# Privacy Policy

**Effective date (entry into force): August 1, 2026**

Service and data operator: the x2proxy brand and the person(s) actually performing the administration, support, compliance control, data processing and provision of access to the x2proxy service, pending possible incorporation and/or publication of other official identification (the “Provider”).

Contacts: privacy@x2proxy.com — privacy matters and legally significant notices; support@x2proxy.com — support, including payment, refund and abuse-related matters; support chat — https://t.me/x2proxysupport; official channel — https://t.me/x2proxy.

User: a natural person, sole proprietor, legal entity or other person using the x2proxy service (the “User”).

This Privacy Policy describes what data may be processed when using the x2proxy service, for what purposes it is used, to whom it may be transferred, and what rights the User has.

By using the Service, the User confirms that they have read this Policy. If applicable law requires separate consent for particular types of processing, such consent is requested separately and this Policy does not replace it.

The Provider may update this Policy. An updated version takes effect on the date specified in it or upon publication in the Service, unless otherwise required by mandatory law.

## 1. GENERAL PROVISIONS

### 1.1. Purpose and status of the Policy

1.1.1. This Privacy Policy governs the collection, use, storage, disclosure, protection and other handling of Users' data when using the x2proxy Service.

1.1.2. The Policy applies to all interactions with the Service, including account registration, use of proxy connections, working through the API, management of sub-accounts, use of the personal dashboard, making payments, receiving bonus traffic, interacting with the Telegram bot, contacting support and receiving notices.

1.1.3. This Policy is an integral part of the terms of use of the Service and applies together with the Terms of Use, the Acceptable Use Policy, the Refund Policy and other documents of the Provider.

### 1.2. Applicable bases for processing

1.2.1. The Provider does not proceed on the basis that any use of the Service automatically constitutes the User's universal consent to all data processing.

1.2.2. Depending on the nature of the processing, the Provider may rely on the necessity of performing a contract, legitimate interests, compliance with applicable law, protection of the Provider's rights, or the User's consent where such consent is required.

1.2.3. If separate consent is required for particular categories of processing or tracking technologies, such consent is requested separately through the relevant interface, settings, banner or other permissible mechanism.

### 1.3. Data-processing principles

1.3.1. The Provider seeks to process data lawfully, fairly and transparently, to the extent reasonably necessary for the operation of the Service, security, performance of contractual obligations and compliance with applicable law.

1.3.2. In processing data, the Provider adheres to the principles of data minimization, purpose limitation, storage limitation, reasonable sufficiency, and confidentiality and integrity of information.

### 1.4. Nature of processing

1.4.1. Data processing may be carried out by automated and non-automated means.

1.4.2. The Provider may carry out the collection, systematization, recording, storage, use, transfer, restriction, deletion, anonymization and other operations with data to the extent necessary to achieve the purposes set out in this Policy.

### 1.5. General reservations

1.5.1. This Policy applies to the maximum permissible extent, taking into account the mandatory rules of applicable law on data protection and electronic communications.

1.5.2. In the event of a conflict between this Policy and mandatory rules of law, such mandatory rules prevail to the relevant extent.

## 2. WHAT DATA WE COLLECT

### 2.1. General scope of data collected

2.1.1. The Provider collects and otherwise processes only those categories of data that are necessary for the operation of the Service, accounting for traffic consumption, security, processing payments, handling requests, analytics, bonus mechanics and compliance with legal requirements.

### 2.2. Categories of data collected

2.2.1. Account data may include the email address, the internal User identifier, the password in the form of a cryptographic hash (where password storage is provided for by the authorization architecture), account settings, data on sub-accounts, API keys, login history, order and purchase history, and other information necessary to administer the Account.

2.2.2. Technical connection and usage data may include the User's IP address, the requester's IP address (client IP), device and browser data, user-agent, operating system, language and regional settings, time zone, session identifiers, login timestamps, connection parameters and technical metadata of interaction with the interface, the API and proxy features.

2.2.3. Proxy-connection logging data may include event identifiers, User and sub-account identifiers, proxy-session and proxy-user identifiers, the request source, the target domain or IP address, the target port, the selected geolocation, timestamps, the request execution status, traffic volume, traffic direction, the client IP address and the proxy IP address.

2.2.4. Payment data may include the wallet address, the transaction identifier (tx hash), the selected network, the amount, the time and status of the transaction, the risk/fraud screening result, the IP address and user-agent at the time of payment, and other limited technical information necessary for crediting funds, billing and risk management.

2.2.5. KYC and restricted-domains data may include the verification status (passed / failed / pending or similar), a service reference ID, limited risk flags, information on the purposes for which the User requests domain unblocking, the list of requested domains and the status of access granted to such domains. The

Provider does not receive the User's full set of documents from the KYC provider, unless expressly stated otherwise.

2.2.6. Support and communications data may include the email address, Telegram username and/or Telegram ID, message content, attachments, screenshots, ticket history, technical logs, information about communication channels, and other data voluntarily provided by the User when contacting support or interacting with the official channels of the service.

2.2.7. Analytics and cookies data may include visit statistics, data on actions within the interface, session data, referral or attribution data, local storage identifiers, pixel-based events, security/anti-fraud signals, and aggregated or pseudonymized metrics of Service use.

2.2.8. Data relating to the Telegram bonus and promo mechanics may include the fact and status of subscription to the Telegram channel, Telegram-bot identifiers, information linking the Telegram interaction with the Account in the Service, and data necessary to prevent repeated or abusive receipt of bonus traffic.

### 2.3. Sources of data

2.3.1. Data may come directly from the User, automatically during use of the Service, from payment and KYC providers, from analytics, support, security and anti-fraud tools, and from complaints, abuse reports or other reports from third parties, where necessary to ensure the operation and security of the Service.

### 2.4. Data minimization

2.4.1. The Provider seeks not to collect excessive data unrelated to the actual operation of the Service or its protection, and limits the scope of processing to the reasonably necessary minimum.

## 3. LOGGING DATA

### 3.1. General provisions

3.1.1. The Provider logs technical parameters of Service use to the extent necessary for accounting for traffic consumption, ensuring security, investigating incidents, preventing abuse and complying with legal requirements.

3.1.2. Logging is technical and operational in nature and is not aimed at analyzing the content of data transmitted by the User.

### 3.2. Composition of logged data

3.2.1. As part of the operation of the Service, the following may be recorded: a unique event identifier; internal user ID; sub-user ID; proxy-session ID; proxy-user ID; source/client IP; target domain or target IP; target port; the selected country, region, state, city or other available geo-parameters; traffic volume; timestamps; status/success/failure; traffic direction; technical connection parameters; the ports used; and other service attributes of the request.

### 3.3. Purposes of using logs

3.3.1. The above data is used to ensure the correct operation of the Service, account for traffic consumption and billing, detect and prevent abuse, ensure the security of the infrastructure, diagnose failures, conduct internal checks, resolve disputes and comply with mandatory legal requirements.

### 3.4. Restrictions on the use of logs

3.4.1. Logs are not used to analyze the content of the User's traffic and are not intended for covert monitoring of the content of network interactions.

3.4.2. The Provider may use technical, behavioral and risk signals for anti-fraud and anti-abuse analysis, but does not carry out covert profiling based on the content of proxied traffic.

### 3.5. Logs of service-infrastructure providers

3.5.1. Certain technical providers ensuring the operation of particular components of the Service may keep their own service logs and use limited data necessary for routing, accounting, security, diagnostics and support of the relevant features. Such processing is limited to standard technical tasks and is carried out to the extent necessary to provide service services to the Provider.

## 4. WE DO NOT STORE TRAFFIC CONTENT

### 4.1. General principle

4.1.1. The Provider does not collect, store or analyze the content of the User's proxied traffic.

4.1.2. Processing is limited to technical connection metadata necessary for routing, usage accounting, security, diagnostics and support of the Service.

### 4.2. What specifically is not stored as traffic content

4.2.1. In the ordinary operation of the Service, the following are not stored: request body/payload; response content; texts of forms and messages transmitted through the proxy; HTML or API content of target resources; page content; credentials transmitted within proxied requests; and other data allowing the actual content of the traffic to be reconstructed.

### 4.3. Transit nature of processing

4.3.1. The Service functions as a mechanism for routing and processing network requests in transit mode, without storing the content of such traffic.

### 4.4. Exceptions

4.4.1. This Section does not apply to data that the User voluntarily submits through registration, payment, support, Telegram-bot, ticketing or other official channels of the Service, since such data does not constitute the content of proxied traffic.

### 4.5. Responsibility for the content of transmitted information

4.5.1. The User is solely responsible for the content of the data it transmits through the Service and for the lawfulness of the relevant usage scenarios.

## 5. PURPOSES AND LEGAL BASES FOR PROCESSING DATA

### 5.1. General provisions

5.1.1. The Provider processes data solely for specified and lawful purposes relating to the provision of the Service, security, analytics, communications, performance of obligations towards the User and compliance with applicable law.

5.1.2. Where required by applicable data-protection law, the legal bases for processing may include the necessity of performing a contract, taking steps prior to entering into a contract at the User's request, the legitimate interests of the Provider and/or third parties, compliance with applicable law, protection of the Provider's rights, and the User's consent where required.

### 5.2. Provision of services and account management

5.2.1. Data is processed to create and maintain the Account, manage sub-accounts, API keys and authorization, provide access to proxy features, route requests, display statistics, apply limits and ensure the operation of the personal dashboard. Where applicable, this basis includes the necessity of performing a contract or taking steps at the User's request prior to entering into it.

### 5.3. Traffic accounting, billing and payments

5.3.1. Data is processed to account for the volume of traffic, manage the balance, apply package validity periods, confirm payments, credit funds, prevent erroneous or suspicious transactions and maintain service records. Where applicable, processing is based on performance of a contract, legitimate interests and/or mandatory legal requirements.

### 5.4. Security, anti-fraud and anti-abuse

5.4.1. Data is processed to protect the Service, the infrastructure, Users and third parties from abuse, fraud, suspicious activity, network attacks, attempts to circumvent restrictions and breaches of the Terms, the AUP and other rules. Where applicable, processing is based on the Provider's legitimate interests and on the necessity of complying with the law and protecting the Provider's rights.

### 5.5. KYC, restricted domains and use-case review

5.5.1. Data is processed to make decisions on access to particular restricted features and domains, conduct KYC, assess the declared use case, manage risks, ensure compliance and restrict impermissible usage scenarios. Where applicable, this basis includes legitimate interests, compliance with law and protection of the Provider's rights and security.

### 5.6. Support and service notices

5.6.1. Data is processed to handle tickets, respond to requests, troubleshoot, and send notices about the account, security, payments, package validity periods, the status of restricted-domain requests, access to features and other mandatory service notices. Such notices are not considered marketing.

### 5.7. Analytics and product development

5.7.1. Data may be processed to analyze use of the Service, improve the interface, test functionality, detect errors and assess the stability and effectiveness of the product. Where required by applicable law, non-essential analytics and similar technologies are activated only after obtaining the relevant consent.

### 5.8. Marketing, community and promo communications

5.8.1. The Provider may use contact data and available communication channels to send marketing messages, product news, promotions, promo offers, messages about the Telegram channel and other communications of an advertising or informational nature. Where required by applicable law, such messages are sent on the basis of prior consent; in other cases the Provider may rely on other legally permissible bases. The User may opt out of marketing messages, but such opt-out does not extend to mandatory service notices.

### 5.9. Law, protection of rights and dispute resolution

5.9.1. Data may be processed to comply with applicable law, interact with competent authorities, fulfil mandatory requests, conduct investigations, protect the Provider's rights, resolve claims and disputes, and establish, exercise and defend legal claims.

### 5.10. Restrictions on the use of data

5.10.1. The Provider does not sell Users' personal data.

5.10.2. The Provider does not use data to analyze the content of proxied traffic and does not build a covert profile of the User based on such content.

5.10.3. The Provider may use limited technical and communication data for access management, security, anti-abuse decisions, communications and promo mechanics, but such processing must remain proportionate to the purposes of the Service.

## 6. KYC AND VERIFICATION

### 6.1. General provisions

6.1.1. The KYC procedure is not mandatory for all Users and is applied at the Provider's discretion, including in cases of suspicious activity, a request for access to restricted domains, an elevated level of risk, a non-standard usage scenario, or financial, reputational or legal risks.

### 6.2. Procedure for conducting KYC

6.2.1. KYC may be carried out through a third-party identification and compliance service. The Provider does not store the full set of documents provided by the User to the external KYC provider, unless expressly required by law or in connection with a separate procedure.

6.2.2. Following such verification, the Provider generally receives a limited set of information: the verification status, a service identifier, individual risk flags, information on the declared use case, and information necessary to decide on access to the requested domains or features.

### 6.3. Restricted domains and use-case review

6.3.1. To open access to particular restricted domains, the Provider may process the User's request, a description of the intended usage scenario, the list of domains, ticket correspondence, the KYC status and the status of previously opened domains.

6.3.2. Such data is used only to decide on granting, restricting or refusing access to the relevant features or domains.

### 6.4. Refusal of KYC

6.4.1. The User may decline to undergo KYC. A refusal of KYC does not, in itself, entail automatic deletion of the account or a complete block of access to the entire Service; however, access to particular restricted functions or restricted domains may be unavailable.

6.4.2. If the User's actions create financial, legal, reputational or other material risks, or there are grounds to believe that the use of the Service violates the rules or the law, the Provider may temporarily freeze the account, restrict particular features, delay consideration of a request or initiate additional verification.

## 7. PAYMENT DATA

### 7.1. General provisions

7.1.1. As of the preparation of this Policy, the Service supports cryptocurrency payment methods through third-party tools and providers that ensure the acceptance, confirmation, analysis and processing of transactions.

7.1.2. The Provider does not store bank-card data and does not obtain access to the User's funds in its wallet.

### 7.2. Categories of payment data

7.2.1. As part of processing cryptocurrency payments, the Provider may record the wallet address, tx hash, network, amount, date and time, transaction status, IP address, user-agent, language parameters, service transaction identifiers, risk assessment and other limited technical information necessary for accounting and payment security.

### 7.3. Purposes of processing payment data

7.3.1. Payment data is processed to confirm and credit a payment, manage the balance, maintain billing, prevent fraud, resolve payment disputes, comply with legal requirements and protect the Provider's rights.

### 7.4. Payment verification and risk management

7.4.1. The Provider may use technical tools and data from payment partners to verify transactions, detect anomalous activity, manage risks and prevent chargeback-like abuse, fraudulent funding, network errors and other anomalies.

7.4.2. If a risk is identified, the Provider may suspend crediting, request additional information, restrict access to the Service or initiate additional verification.

### 7.5. Retention periods and transfer

7.5.1. Payment metadata is stored for the period specified in this Policy and may be transferred to payment, analytics and compliance services to the extent necessary for processing the transaction, risk verification, accounting and compliance with the law.

### 7.6. Limitation of liability

7.6.1. Payment operations via the blockchain and external services depend on the selected network, confirmations, the stability of third-party tools and the correctness of the User's own actions. The terms of processing such transactions may additionally be governed by the rules of the relevant services.

## 8. COOKIES, ANALYTICS AND TELEGRAM INTEGRATIONS

### 8.1. Technologies used

8.1.1. The Service may use cookies and similar technologies, including strictly necessary cookies, auth/session cookies, preference cookies, analytics cookies, security cookies, referral or attribution identifiers, local storage, pixels, technical anti-fraud scripts and other similar means used for the operation, analysis and protection of the Service.

8.1.2. Depending on the Service configuration, both first-party and third-party analytics tools, product analytics, attribution, performance tracking and, where necessary, advertising or marketing pixels may be used.

### 8.2. Purposes of using cookies and analytics

8.2.1. Such technologies may be used for authentication, session management, saving settings, ensuring security, protecting against abuse, analyzing interface use, improving functionality, diagnosing errors, and measuring the effectiveness of traffic sources and communications.

### 8.3. Consent and preference management

8.3.1. Strictly necessary and other technologies whose use is permitted without separate consent may be applied automatically to the extent permitted by law.

8.3.2. Analytics, marketing and other non-essential technologies are enabled only where the User's consent is present in cases where such consent is required by applicable law. For this purpose, the Service may use a cookie banner, consent manager, preference center or similar settings-management mechanism.

8.3.3. The User may at any time change cookie settings through an available interface, browser settings or other management tools, where available in the specific Service configuration.

### 8.4. Third-party analytics and marketing tools

8.4.1. Depending on the product configuration, the Provider may use self-hosted analytics, solutions similar to Google Analytics, product analytics tools, event-tracking systems, advertising and attribution tools, and other technical means of analysis or communication. The specific list of tools used may change.

8.4.2. The Provider seeks to limit the amount of data transferred to such tools, to use aggregated, pseudonymized or otherwise minimized data where possible, and not to use such tools to analyze the content of proxied traffic.

### 8.5. Telegram bonus and Telegram bot

8.5.1. To provide bonus traffic associated with subscription to the Telegram channel, the Provider may use a Telegram bot and other Telegram integrations.

8.5.2. As part of such mechanics, the following may be processed: Telegram username, Telegram ID, the fact and status of subscription to the channel, technical information about interaction with the bot, information linking the Telegram account with the account in the Service, and data necessary to prevent repeated or abusive receipt of the bonus.

8.5.3. Telegram-integration data may be used to confirm fulfilment of the bonus conditions, maintain communication channels with the User, account for communication sources, prevent abuse and provide additional notices about the operation of the Service.

8.5.4. The User's interaction with Telegram is also governed by Telegram's own policies and rules, which the Provider cannot fully influence.

### 8.6. Retention periods

8.6.1. The retention period for cookies and related analytics data depends on the category of technology and its purpose. Strictly necessary cookies may be stored for the duration of the session or another period reasonably necessary for the operation of the Service; analytics and similar data, unless otherwise specified in the particular interface, is stored within the periods specified in this Policy, or for another shorter or longer period where justified by the cookie category, legitimate security interests or legal requirements.

## 9. DATA RETENTION PERIODS

### 9.1. General provisions

9.1.1. The Provider stores data for the period necessary to achieve the purposes of processing, ensure security, resolve disputes, prevent abuse and comply with legal requirements.

### 9.2. Baseline retention periods

9.2.1. Unless a different period is required by law, a separate procedure or a legal hold, the following indicative retention periods apply: (a) logging data, technical connection data, security and anti-abuse logs — up to 730 days; (b) payment metadata, transaction information and other payment-related logs — up to 365 days; (c) cookies and analytics data — up to 180 days, unless otherwise determined by the cookie category or the settings of a specific tool; (d) support tickets, messages and other communications with the User — up to 365 days.

9.2.2. Account data may be stored for the duration of the account and a reasonable period after its deletion, to the extent necessary for billing, security, abuse prevention, dispute resolution, compliance and protection of the Provider's rights.

### 9.3. Extension of retention periods

9.3.1. The Provider may extend the retention period for particular data where there is a dispute, investigation, internal check, legal hold, law-enforcement request, compliance requirement, need to protect the Provider's rights, need to prevent abuse or other reasonable security grounds.

### 9.4. Deletion and anonymization

9.4.1. Upon expiry of the applicable period, data is deleted, de-identified or anonymized within a reasonable time, where its further storage is not required by law or for a protected purpose.

### 9.5. Retention after account deletion

9.5.1. Deletion of an account does not mean immediate deletion of all data. Certain categories of data, including logs, security, billing and messaging data and other service records, may be retained within the established periods and for purposes permitted by law.

## 10. DISCLOSURE OF DATA

### 10.1. General provisions

10.1.1. The Provider may disclose the User's data only in cases expressly provided for by this Policy, by applicable law, by requests from competent authorities, by mandatory decisions, and where necessary to protect the rights, interests and security of the Provider, Users, third parties or the Service infrastructure.

### 10.2. Grounds for disclosure

10.2.1. Data may be disclosed: (a) upon a lawful and duly formalized request from a governmental, judicial or other authorized body; (b) to prevent, investigate or suppress fraud, abuse, breaches of the Terms/AUP, security threats or other unlawful actions; (c) to protect the rights and legitimate interests of the Provider; (d) where necessary to perform a contract or ensure the operation of particular components of the Service; (e) in other cases permitted by law.

### 10.3. Scope of disclosure

10.3.1. When disclosing data, the Provider proceeds on the principle of minimization and transfers only the amount of information that is objectively necessary to achieve the relevant purpose.

10.3.2. As a general rule, disclosure may include technical logs, IP addresses, timestamps, action statuses, service identifiers, payment metadata, KYC status, support records and other limited technical or accounting information.

10.3.3. The Provider does not disclose the content of proxied traffic, since such data is not collected or stored in the ordinary operation of the Service.

### 10.4. Assessment of requests and notification

10.4.1. The Provider may assess the lawfulness and validity of incoming requests and, where permitted by law, restrict or reject excessive, vague or unverified requests.

10.4.2. Notification of the User about a disclosure may not be carried out where this is prohibited by law, may impede an investigation, create a security risk or otherwise conflict with the protected purpose of the disclosure.

## 11. THIRD PARTIES AND INTERNATIONAL TRANSFERS

### 11.1. Categories of third parties

11.1.1. For the operation of the Service, the Provider may engage third-party providers of technical, payment, compliance, analytics, communication, helpdesk, security and other service services.

11.1.2. Such categories may include, in particular: payment and transaction services; KYC and compliance vendors; technical, network, infrastructure and security providers; analytics and product analytics providers; providers of email, messaging, ticketing and other communication channels; professional advisers; and authorities and other persons to whom data must be disclosed by law.

### 11.2. Scope of processing by third parties

11.2.1. Such persons receive only the data necessary to perform the relevant function. Depending on the category of provider, this may be account data, billing data, connection metadata, support data, Telegram-related identifiers, analytics signals, KYC status, risk-related signals and other service information.

11.2.2. Certain technical providers ensuring the operation of particular components of the Service may see limited account, billing, usage and logging data necessary for the functioning of the relevant technical solutions.

### 11.3. International transfers

11.3.1. Since the Service may use providers and tools located in various countries, data may be processed and transferred outside the User's country or the country from which access to the Service is made.

11.3.2. The level of data protection in such jurisdictions may differ from the level of protection in the User's country. Where applicable, the Provider seeks to use reasonable contractual, technical and organizational measures, and other legally permissible mechanisms, to protect data in cross-border transfers.

### 11.4. Restrictions on the use of data by third parties

11.4.1. The Provider seeks to engage counterparties that undertake to use data only to provide the relevant services to the Provider or in other cases expressly permitted by law or by their own role in the processing.

11.4.2. The specific set of such providers and services may change without prior notice to the User.

## 12. DATA SECURITY AND AUTOMATED CHECKS

### 12.1. Technical and organizational measures

12.1.1. The Provider takes reasonable technical and organizational measures to protect data against unauthorized access, loss, alteration, disclosure or destruction, taking into account the nature of the data, the structure of the Service and the level of risk.

12.1.2. Such measures may include encryption in transit, access segregation, authentication, logging of administrative actions, infrastructure segmentation, redundancy, monitoring of security events, the use of anti-fraud tools and other measures appropriate to the current needs of the Service.

### 12.2. Limitations and risks

12.2.1. The transmission of data over the internet and the use of a distributed technical infrastructure inherently involve certain risks. The Provider does not guarantee the absolute security of the data-transmission environment, but seeks to take measures proportionate to the risks.

### 12.3. Automated signals and risk assessment

12.3.1. The Provider may use automated signals, behavioral rules, anomaly detection, risk scoring, fraud flags and other means of technical assessment of Users' activity for the purposes of security, anti-abuse, protection of the infrastructure and management of access to particular features.

12.3.2. Such mechanisms may result in a temporary account freeze, restriction of particular features, initiation of a check, a KYC request, a delay in granting access to restricted domains, or referral of a request for additional review.

12.3.3. Where applicable law grants the User additional safeguards in respect of decisions based solely on automated processing, the Provider seeks to ensure appropriate procedures, including the possibility of additional review with human involvement where required.

### 12.4. Security incidents

12.4.1. Upon detection of security incidents, the Provider may take the necessary measures, including restricting access, conducting internal checks, interacting with providers and competent authorities, and taking other steps aimed at minimizing consequences and preventing recurrence.

## 13. USER RIGHTS

### 13.1. General provisions

13.1.1. The User has rights in relation to its data to the extent provided by applicable data-protection law.

### 13.2. Possible rights

13.2.1. Depending on applicable law, the User may have the right to information about processing, access to data, rectification, erasure, restriction of processing, data portability, objection to processing, withdrawal of consent, lodging a complaint with a supervisory authority, and the right not to be subject to a decision based solely on automated processing, where such a right is provided by law.

### 13.3. Procedure for submitting requests

13.3.1. To exercise these rights, the User may send a request to privacy@x2proxy.com or through other official communication channels specified in the Service. The Provider may request additional information necessary to identify the User and prevent unauthorized disclosure of data.

### 13.4. Time frames for handling requests

13.4.1. The Provider handles privacy requests without undue delay and, as a general rule, seeks to respond within 30 calendar days, unless a different period is established by applicable law.

13.4.2. If a request is complex, voluminous, repetitive or requires additional verification, the response period may be extended to the extent permitted by applicable law. Where necessary, the User is notified of such an extension.

### 13.5. Limitations on fulfilling requests

13.5.1. The Provider may refuse to fulfil a request in whole or in part, or limit the amount of information provided, where this is permitted by law, infringes the rights of third parties, jeopardizes the security of the Service, impedes an investigation, or where the relevant data must be retained for legal, compliance, billing, fraud-prevention or security reasons.

## 14. CHANGES TO THE POLICY

### 14.1. Right to make changes

14.1.1. The Provider may update this Policy in light of the development of the Service, changes to its functionality, the introduction of new technologies, and changes to payment methods, communications, analytics, legislation and security requirements.

### 14.2. Entry of changes into force

14.2.1. An updated version takes effect on the date specified in such version or upon publication, unless otherwise provided by applicable law.

14.2.2. For significant changes, the Provider may use notices in the interface, by email, in official messengers or through other available communication channels.

14.2.3. If new consent is required for a particular category of processing or communication, the Provider requests it separately and does not treat continued use of the Service as a universal substitute for such consent where this is prohibited by law.

## 15. CONTACTS

### 15.1. Communication channels

15.1.1. On matters of privacy, data processing, the exercise of rights and other privacy matters, the User may contact privacy@x2proxy.com.

15.1.2. On general matters relating to use of the Service, the User may contact the Provider through the official email, a support form, the built-in ticketing system, official Telegram or other messengers specified in the Service interface or on official resources.

15.1.3. The Provider may update the list of available communication channels as the Service develops.

### 15.2. Communications with the User

15.2.1. The Provider may send the User service, technical, billing, security, KYC, restricted-domain, support and other mandatory messages via email, the personal dashboard, Telegram, messengers and other available channels.

15.2.2. Marketing and promo communications may be sent to the extent and on the grounds permitted by law. The User may opt out of marketing messages, but such opt-out does not affect the receipt of mandatory service notices.

### 15.3. Electronic form of interaction

15.3.1. The User agrees that interaction with the Provider on matters relating to the Service and this Policy may be carried out in electronic form.