OSTNYX

a platform operated by Ostora Group

PRIVACY POLICY

Including Call Monitoring, Call Recording, and Platform Monitoring Disclosures

Ostora Group BV
Lange van Bloerstraat 51, 2060 Antwerpen, Belgium
info@ostora.be · ostnyx.com
Chairman: Muneeb ur Rehman · Chief Executive Officer: Haseeb Ali

Version 1.0 — Effective 1 August 2026

Table of Contents

1. Introduction and Scope

This Privacy Policy ("Policy") describes how Ostora Group BV, a company organized under the laws of Belgium with its registered office at Lange van Bloerstraat 51, 2060 Antwerpen, Belgium ("Ostora Group," "Ostnyx," "we," "us," or "our"), collects, uses, discloses, retains, and protects personal data in connection with the Ostnyx platform available at ostnyx.com and any associated applications, dashboards, APIs, and services (collectively, the "Service").

Ostnyx is a business communications and lead-management platform that enables organizations and individual users ("Users," "you," or "your") to place and receive telephone calls, send and receive text messages, manage sales leads, and monitor the calling activity of their staff and team members through the Service.

Because the Service is fundamentally built around telephone calling, messaging, and the management of personnel who place calls on behalf of organizations, the scope of data collection, monitoring, and retention described in this Policy is more extensive than what a purely informational website or consumer application would typically disclose. We ask that you read this Policy carefully, in particular Sections 7, 8, and 9, before using the Service.

This Policy applies to all Users of the Service, including individual account holders, employees or contractors of an organization using the Service ("Team Members"), and administrators of an organization's Ostnyx account ("Administrators"). It also applies, to the extent described in Section 5, to individuals whose personal data is processed through the Service as leads, contacts, or call recipients, even though such individuals are not themselves Users.

This Policy should be read together with the Ostnyx Terms of Service and, where applicable, any Data Processing Agreement entered into between Ostora Group and an organizational customer. In the event of a conflict between this Policy and a signed Data Processing Agreement with a specific customer, the terms of that Data Processing Agreement shall prevail with respect to that customer's data.

By creating an account, accessing, or otherwise using the Service, you acknowledge that you have read and understood this Policy. If you do not agree with any part of this Policy, you must not use the Service.

1.1 Purpose Statement

Ostora Group's overarching purpose in publishing this Policy is twofold: first, to give Users, Team Members, Administrators, and call recipients a clear and complete understanding of how their personal data is collected, used, and, where applicable, monitored; and second, to set out, in a single reference document, the safeguards, rights, and accountability mechanisms Ostora Group has put in place consistent with the GDPR and other applicable data protection and telecommunications law. Ostora Group is committed to processing personal data lawfully, fairly, and transparently, and to applying the principles of data minimization, purpose limitation, and accountability set out in Article

5 of the GDPR to the extent consistent with the fraud-prevention and platform-integrity objectives described in Section 7.

2. Definitions

- "Administrator" means a User with elevated permissions to manage an organization's Ostnyx account, including the ability to access call recordings, message content, and usage data of Team Members within that organization.
- "Call Data" means information generated in connection with a telephone call placed or received through the Service, including but not limited to the numbers involved, timestamps, duration, call outcome, notes, and any audio recording of the call.
- "Controller" has the meaning given in Article 4(7) of the GDPR: the entity that determines the purposes and means of the processing of personal data.
- "Fraudulent Activity" means any use of the Service to facilitate deception, misrepresentation, unauthorized solicitation, scam calling or messaging campaigns, or other unlawful conduct directed at call or message recipients.
- "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
- "Lead Data" means personal data relating to a prospective or existing customer of a User, including contact details, notes, and interaction history, that is stored, imported, or managed within the Service.
- "Personal Data" means any information relating to an identified or identifiable natural person, as defined in Article 4(1) of the GDPR.
- "Processor" has the meaning given in Article 4(8) of the GDPR: an entity that processes personal data on behalf of a Controller.
- "Recording" means an audio capture of a telephone call placed or received through the Service, stored by or on behalf of Ostora Group.
- "Sub-processor" means a third-party processor engaged by Ostora Group to process personal data on our behalf in connection with the Service.
- "Special Category Data" means personal data revealing racial or ethnic origin, political opinions, religious beliefs, health data, or other categories of data described in Article 9 of the GDPR.
- "Supervisory Authority" means an independent public authority responsible for monitoring the application of the GDPR, such as the Belgian Data Protection Authority.
- "Team Member" means an individual User operating under the account of an Administrator or organization.
- "Wallet" means the prepaid balance maintained within a User's Ostnyx account, used to pay for numbers, calls, and messages.

3. Data Controller Information

The data controller responsible for the processing of personal data described in this Policy is:

Ostora Group BV

Registered address: Lange van Bloerstraat 51, 2060 Antwerpen, Belgium

Email: info@ostora.be

Website: ostnyx.com

Chairman: Muneeb ur Rehman

Chief Executive Officer: Haseeb Ali

Data protection enquiries may be directed to the contact point identified in Section 24. Ostora Group has assessed that, given the current scale and nature of its processing activities, the formal appointment of a statutory Data Protection Officer under Article 37 of the GDPR is not presently mandatory; this assessment is reviewed periodically as the Service and its user base grow.

4. Roles and Responsibilities: Controller and Processor

The processing of personal data through the Service involves multiple parties acting in different capacities depending on the data category and processing activity concerned. This Section clarifies those roles.

Data / Activity	Ostora Group's Role	Organization's Role (where applicable)
Account creation, billing, wallet and platform-security data	Controller	N/A
Call recordings and Call Data generated by an organization's Team Members	Processor	Controller
Message content sent by an organization's Team Members	Processor	Controller
Lead Data imported or managed by an organization	Processor	Controller
Fraud-prevention and platform-integrity monitoring (Section 7)	Controller (independent legitimate interest)	Joint interest, where organization also monitors
Administrator-level monitoring of Team Members	Processor (infrastructure only)	Controller (decides scope and use of monitoring)

Where Ostora Group acts as a processor on behalf of an organizational customer, that organization is responsible, as controller, for ensuring it has a valid legal basis for the collection and monitoring of its Team Members' and leads' personal data, for providing any required notices to those individuals (including Team Members and call recipients), and for responding to data subject requests in the first instance, with Ostora Group providing reasonable assistance as required under Article 28 of the GDPR.

Where Ostora Group acts as controller — including in respect of platform-wide fraud-prevention monitoring described in Section 7, which Ostora Group carries out in its own right regardless of any

organization's separate monitoring — Ostora Group is directly responsible for compliance with the GDPR in respect of that processing.

5. Categories of Personal Data We Collect

5.1 Account and Identity Data

Name, email address, phone number, billing address, username, password (stored in hashed form), and profile information you provide when creating or managing your account.

5.2 Call Data

When a call is placed or received through the Service, we collect and store, at minimum: the origin and destination numbers, timestamps, duration, billed seconds, cost, call outcome, and any notes entered by the User. Where call recording is enabled — whether by default organizational policy or Administrator configuration — we additionally collect and store the full audio recording of the call, including the voices of both the User and the call recipient.

5.3 Messaging Data

Where the Service is used to send or receive SMS or other text messages, we collect and store the full content of such messages, sender and recipient numbers, timestamps, and delivery status.

5.4 Platform Usage and Technical Data

Login timestamps, session duration, features accessed, pages viewed, click and navigation events, device type, operating system, browser type, IP address, and approximate geographic location derived from IP address.

5.5 Lead and Contact Data

Names, phone numbers, email addresses, business names, notes, statuses, and other information relating to leads or contacts that Users create, import (including via Google Sheets or similar integrations), acquire from shared lead pools, or otherwise manage within the Service.

5.6 Payment Data

Billing name, billing address, and payment method details. Full payment card numbers are collected and processed by our payment processor, Stripe, and are not stored on Ostnyx's own systems. We retain records of transactions, invoices, and wallet balances.

5.7 Administrator and Team Monitoring Data

Where a User operates under an organizational account, the Administrator(s) of that account may access: the User's call recordings and Call Data; the content of the User's message threads sent through the Service; the User's login activity, session data, and feature usage; and the User's lead

pipeline, call outcomes, and performance metrics. This monitoring capability is a core, disclosed function of the Service and is described further in Sections 7 and 8.

5.8 Voice Demo and Recruitment Data

Where the Service is used for recruitment or vetting purposes, we may collect voice recordings, application responses, and related qualification information submitted by applicants through public-facing forms.

5.9 Special Category Data

Ostora Group does not intentionally request or require Users to submit Special Category Data. However, because Call Data and Messaging Data may capture the full content of a conversation or message exchanged between a User and a third party, it is possible that such content could incidentally reveal Special Category Data about the User, a Team Member, or a call/message recipient (for example, where health, religious, or similar information is mentioned during a call). Where this occurs, such data is processed on the same legal bases and subject to the same safeguards described in this Policy, and is not used by Ostora Group for any purpose other than those described in Sections 7 and 10. Users must not deliberately solicit or record Special Category Data from call recipients except where strictly necessary for a legitimate business purpose and in compliance with Article 9 of the GDPR.

6. Legal Bases for Processing

We process personal data on the following legal bases under Article 6 of the GDPR:

Processing Purpose	Legal Basis
Providing the core calling, messaging, and lead-management Service	Performance of a contract (Art. 6(1)(b))
Billing, invoicing, and payment processing	Performance of a contract; legal obligation (Art. 6(1)(b), (c))
Call and message monitoring by Administrators	Legitimate interests of the organization; performance of a contract (Art. 6(1)(b), (f))
Fraud prevention and platform-integrity monitoring	Legitimate interests; legal obligation where applicable (Art. 6(1)(f), (c))
Responding to lawful requests from authorities	Legal obligation (Art. 6(1)(c))
Marketing communications (where applicable)	Consent, or legitimate interests for existing customers (Art. 6(1)(a), (f))
Service improvement, analytics, and troubleshooting	Legitimate interests (Art. 6(1)(f))

Where processing relies on legitimate interests, we have assessed that our interests — and, in the case of Administrator monitoring, the interests of the relevant organization — are not overridden by the interests or fundamental rights of the individuals concerned, taking into account the business and security context in which the Service operates. This assessment is documented internally and is available to the competent supervisory authority upon lawful request.

7. Why We Monitor: Fraud Prevention and Platform Integrity

Ostnyx enables Users to place a high volume of outbound telephone calls and text messages, including to members of the public who are not themselves Users of the Service. Communications platforms of this kind are, by their nature, attractive targets for misuse, including fraudulent calling operations, scam campaigns, unauthorized robocalling, and other deceptive or illegal practices carried out by bad-faith Users.

As the operator of the underlying infrastructure through which such calls and messages are placed, Ostora Group may bear legal, regulatory, reputational, and contractual responsibility — including potential liability to telecommunications carriers, payment processors, regulators, and members of the public — if the Service is used to facilitate fraud, scams, or other unlawful conduct, whether or not Ostora Group had direct knowledge of the specific misuse. This is the central reason Ostnyx implements comprehensive platform monitoring, notwithstanding the more extensive data collection this entails compared to a purely conversational or social application.

For this reason, Ostnyx implements comprehensive monitoring of platform activity, including but not limited to:

- Recording and reviewing calls placed through the Service, where recording is enabled;
- Reviewing the content of messages sent through the Service;
- Monitoring call volume, calling patterns, and destination numbers for indicators of fraud, spam, or abuse;
- Monitoring account activity, login patterns, and payment behavior for indicators of unauthorized access or payment fraud;
- Cross-referencing User activity against known fraud indicators and, where applicable, industry blocklists;
- Suspending, restricting, or terminating accounts, and reporting activity to relevant authorities or carriers, where fraud or misuse is reasonably suspected.

This monitoring is carried out both by Ostora Group directly and, where an organizational account is in use, by that organization's Administrators. Monitoring for these purposes is carried out on the legal bases described in Section 6, principally our legitimate interest — and, where an organization is the relevant controller, that organization's legitimate interest — in preventing fraud, protecting the integrity of the Service, complying with legal and regulatory obligations, and avoiding liability arising from misuse of the Service by third parties.

Ostora Group has considered less intrusive alternatives to comprehensive monitoring, including sampling-based review and metadata-only analysis, and has determined that, given the volume and international scope of calling activity conducted through the Service, full monitoring capability is proportionate and necessary to meet the fraud-prevention and platform-integrity objectives described in this Section, while access to recorded content is restricted as described in Section 8.3.

By using the Service, you acknowledge and accept that your calls, messages, and platform activity are subject to this level of monitoring for the purposes described in this Section.

8. Call Recording, Monitoring, and Notice Requirements

Calls placed or received through the Service may be recorded and/or monitored in real time, for the purposes described in Sections 7 and 10, including quality assurance, staff training, dispute resolution, fraud prevention, and legal compliance.

8.1 Notice to Call Recipients

Where a call is recorded or monitored, and where required by applicable law, an audible notice, tone, or verbal disclosure will be provided to indicate that the call is being recorded or monitored. The specific consent requirements for call recording vary significantly by jurisdiction; a non-exhaustive illustrative summary is provided at Annex A. Consent and notice requirements should always be confirmed against current local law, as they are subject to change.

8.2 Responsibility of the Account Holder

Ostora Group provides the technical infrastructure that enables call recording and monitoring. The User and, where applicable, the Administrator or organization operating the account, are responsible for configuring and using this functionality in a manner that complies with the call-recording and consent laws applicable in each jurisdiction from which, and to which, calls are placed. This includes ensuring that any required notice or consent is actually given to call recipients before or at the start of a recorded call.

Ostora Group disclaims liability for a User's failure to comply with applicable call-recording consent laws, without prejudice to any obligations Ostora Group has as a data processor under the GDPR or other applicable data protection law.

8.3 Access to Recordings

Call recordings may be accessed by: the User who placed or received the call; the Administrator(s) of the organizational account under which the call was placed; and authorized Ostora Group personnel, for support, security, fraud-investigation, and legal-compliance purposes. Access is logged and restricted to personnel and Administrators with a legitimate need to access such recordings.

9. Acceptable Use of the Service and User Obligations

In consideration of the extensive monitoring described in Sections 7 and 8, and to protect Ostora Group, other Users, and members of the public, all Users agree to the following obligations when using the Service:

- Users must not use the Service to place calls or send messages for any fraudulent, deceptive, or unlawful purpose, including impersonation, phishing, or unauthorized solicitation;

- Users must not use the Service to conduct unsolicited automated or "robocall" campaigns that violate applicable telemarketing, consumer-protection, or telecommunications law;
- Users must obtain and provide any consent or notice required by the law of the jurisdiction in which a call recipient is located before recording a call, as described in Section 8;
- Users must not use the Service to harass, threaten, or repeatedly contact individuals who have requested no further contact;
- Users, where acting as Administrators, must inform their own Team Members that their calls, messages, and platform activity will be monitored and, where required by local employment or data protection law, obtain any necessary consent or provide any necessary notice to those Team Members;
- Users must not attempt to circumvent, disable, or interfere with the monitoring, recording, or security functionality of the Service;
- Users must promptly report any suspected fraudulent use of the Service, whether by themselves, their Team Members, or third parties, to info@ostora.be.

Violation of these obligations may result in suspension or termination of the User's account, removal of content, reporting to relevant telecommunications carriers or authorities, and, where applicable, legal action. These obligations are without prejudice to any more detailed obligations set out in the Ostnyx Terms of Service or Acceptable Use Policy. Illustrative indicators that may trigger a fraud or abuse review are set out at Annex C.

9.1 Confidentiality Obligations of Ostora Group Personnel

All Ostora Group personnel, contractors, and Administrators with access to call recordings, message content, or other personal data processed through the Service are bound by confidentiality obligations, whether contractual or statutory, restricting their use of such data to the legitimate purposes described in this Policy. Access to recordings and message content by Ostora Group personnel is limited to those with a demonstrated operational need, such as support, fraud investigation, or legal compliance, and is logged in accordance with Section 16.

10. How We Use Your Information

In addition to the purposes described above, we use personal data collected through the Service to:

- Provide, operate, maintain, and improve the Service, including the dialer, messaging, lead-management, and analytics functionality;
- Process payments, manage wallet balances, and issue invoices;
- Provision and manage telephone numbers on behalf of Users, including through our telecommunications carriers;
- Enable Administrators to monitor and manage the performance of Team Members;
- Detect, investigate, and prevent fraud, abuse, and violations of our Acceptable Use Policy or Terms of Service;

- Respond to support requests and communicate with Users about their account or the Service;
- Comply with applicable legal, regulatory, tax, and accounting obligations;
- Respond to lawful requests from courts, law enforcement, or regulatory authorities;
- Where consented to, or otherwise permitted, send marketing or product update communications.

11. Automated Processing and Profiling

The Service may use automated rules and, in certain features, algorithmic or AI-assisted processing to: flag calling patterns that may indicate fraud or abuse; automatically release inactive leads back into a shared pool according to configured time thresholds; suspend numbers with unpaid balances; and reconcile payments and carrier rates.

These automated processes do not, on their own, produce legal effects or similarly significant effects on individuals within the meaning of Article 22 of the GDPR. Where any automated decision-making with such effects is introduced in the future, we will update this Policy and provide the information required by Article 22 GDPR, including the right to obtain human intervention.

12. Cookies and Tracking Technologies

The Service and the ostnyx.com website use cookies and similar tracking technologies to operate core functionality (such as maintaining a logged-in session), remember preferences, and analyze usage of the Service. Categories of cookies used include:

Category	Purpose
Strictly necessary	Session management, authentication, security
Functional	Remembering User preferences and settings
Analytics	Understanding how the Service is used, in aggregate, to improve it

Where required by applicable law, we will request your consent to non-essential cookies through a cookie-consent mechanism on the website. You may control cookies through your browser settings, although disabling certain cookies may affect the functionality of the Service.

13. Data Sharing and Sub-Processors

We share personal data with the following categories of third-party service providers, each acting as a sub-processor engaged to support the operation of the Service. We have entered into, or will enter into, Data Processing Agreements with each sub-processor that processes personal data on our behalf, as required by Article 28 of the GDPR. A more detailed register of current sub-processors is provided at Annex B.

Sub-processor Category	Purpose
Telecommunications carrier(s)	Call routing, number provisioning, SMS delivery
Call-routing infrastructure provider	Call bridging and routing infrastructure
Payment processor	Payment processing
Cloud hosting and database provider	Application hosting, data storage

We do not sell personal data, call recordings, or message content to third parties for advertising or marketing purposes. We may disclose personal data where required to comply with a legal obligation, court order, or lawful request from a government or regulatory authority, or where necessary to protect the rights, property, or safety of Ostora Group, our Users, or the public, including in connection with the fraud-prevention purposes described in Section 7.

In the event of a merger, acquisition, restructuring, or sale of assets involving Ostora Group or Ostnyx, personal data may be transferred to the acquiring or resulting entity, subject to the protections described in this Policy. We will provide notice of any material change in sub-processors in accordance with the update mechanisms described in Section 22.

13.1 Cooperation with Law Enforcement and Carriers

Ostora Group may cooperate with telecommunications carriers, payment processors, and law enforcement or regulatory authorities investigating suspected fraud, abuse, or unlawful use of the Service, including by providing Call Data, message metadata, or account information in response to a lawful request, consistent with Section 7 and applicable law. Where legally permitted, Ostora Group will assess such requests for validity and proportionality before disclosure.

14. International Data Transfers

Ostnyx operates internationally and may transfer personal data to countries outside the European Economic Area ("EEA"), including in connection with telecommunications carriers and infrastructure providers located outside the EEA. Where such transfers occur, we rely on appropriate safeguards recognized under the GDPR, including the European Commission's Standard Contractual Clauses, adequacy decisions, or other lawful transfer mechanisms, to ensure that transferred personal data continues to benefit from a level of protection essentially equivalent to that guaranteed within the EEA.

Where a User places calls to, or receives calls from, a jurisdiction outside the EEA, the personal data exchanged in that call (including any recording) will necessarily be accessible from that jurisdiction as an inherent feature of international telephony, independent of the safeguards described above, which apply to Ostora Group's own storage and processing infrastructure.

15. Data Retention Schedule

We retain personal data for no longer than is necessary for the purposes described in this Policy, taking into account legal, accounting, and reporting requirements. The following table sets out our standard retention periods; specific periods may vary based on organizational configuration or legal requirements.

Data Category	Standard Retention Period
Call recordings	[X] months from the date of the call, unless retained longer for an active dispute, investigation, or legal obligation

Message content	[X] months from the date of the message
Call and message metadata	Duration of the account, plus [X] years thereafter
Account and billing records	7 years, in accordance with Belgian accounting and tax law
Lead and contact data	Duration of the account, or until deletion is requested
Platform usage and technical logs	Up to 12 months
Voice demo / recruitment submissions	Up to 12 months from submission, or as otherwise agreed with the applicant

Upon closure of an account, we will delete or anonymize personal data in accordance with this schedule, except where retention is required to comply with a legal obligation, resolve a dispute, enforce our agreements, or fulfil the fraud-prevention purposes described in Section 7.

16. Data Security Measures

We implement technical and organizational measures designed to protect personal data against unauthorized access, alteration, disclosure, or destruction, including:

- Encryption of data in transit and, where applicable, at rest;
- Access controls restricting Administrator and staff access to personal data on a need-to-know basis, with access logging;
- Hashed storage of account passwords;
- Segregation of duties between Ostora Group personnel and organizational Administrators;
- Regular review of access permissions and security configurations;
- Contractual security obligations imposed on sub-processors.

No system of transmission or storage can be guaranteed to be 100% secure. In the event of a security incident affecting personal data, we will act in accordance with the breach notification procedure described in Section 17.

16.1 Data Protection by Design and Default

Consistent with Article 25 of the GDPR, Ostora Group seeks to implement data protection by design and by default when developing new features of the Service, including by limiting default data-sharing settings, restricting Administrator visibility to data reasonably necessary for the monitoring purposes described in this Policy, and considering the data-protection impact of new functionality before release. This principle is applied to the extent consistent with the fraud-prevention and platform-integrity objectives described in Section 7, which by their nature require broader access than a strict data-minimization default would otherwise suggest.

17. Data Breach Notification Procedure

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, Ostora Group will, without undue delay and, where feasible, within 72 hours of becoming aware of the breach, notify the competent supervisory authority in accordance with Article 33 of the GDPR.

Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, we will also notify those individuals without undue delay, in accordance with Article 34 of the GDPR, describing the nature of the breach, its likely consequences, and the measures taken or proposed to address it.

Where Ostora Group processes personal data as a processor on behalf of an organizational customer, we will notify that customer without undue delay upon becoming aware of a personal data breach, to enable the customer to fulfil its own notification obligations as controller.

17.1 Internal Escalation

Suspected security incidents identified by any Ostora Group personnel, Administrator, or User must be reported immediately to info@ostora.be. Upon receipt, the incident is triaged to determine scope, affected data categories, and affected individuals, and the notification timelines described above are calculated from the point at which Ostora Group first becomes aware of the incident, consistent with Article 33 GDPR.

18. Your Rights Under the GDPR

If you are located in the EU/EEA, or your personal data is otherwise subject to the GDPR, you have the following rights in relation to your personal data, subject to the conditions and exceptions set out in applicable law:

- Right of access — to obtain confirmation of whether we process your personal data, and a copy of that data (Art. 15);
- Right to rectification — to have inaccurate or incomplete personal data corrected (Art. 16);
- Right to erasure — to request deletion of your personal data, subject to legal retention requirements (Art. 17);
- Right to restriction of processing — to request that we limit how we use your data in certain circumstances (Art. 18);
- Right to data portability — to receive certain personal data in a structured, commonly used, machine-readable format (Art. 20);
- Right to object — to object to processing based on legitimate interests, including profiling, and to direct marketing at any time (Art. 21);
- Right to withdraw consent — where processing is based on consent, at any time, without affecting the lawfulness of processing before withdrawal (Art. 7(3));
- Right to lodge a complaint — with the Belgian Data Protection Authority (Gegevensbeschermingsautoriteit / Autorité de protection des données) or the supervisory authority of your habitual residence.

18.1 How to Submit a Request

To exercise any of these rights, please email info@ostora.be with the subject line "Data Subject Request," describing the right you wish to exercise and providing sufficient information to verify your identity. We may request additional information to confirm your identity before processing a request.

Step	Description	Typical Timeframe
1. Submission	Request received at info@ostora.be	—
2. Identity verification	We confirm the requester's identity and account	Up to 5 business days
3. Assessment	We determine the applicable controller/processor role (Section 4) and applicable exceptions	Up to 10 business days
4. Response	We provide a substantive response or requested data	Within 1 month of receipt (extendable by up to 2 further months for complex requests, with notice)

Where a request relates to Call Data, Lead Data, or other personal data that an organizational Administrator controls, we may direct your request to the relevant Administrator or process it jointly with that organization, consistent with the controller/processor relationship described in Section 4.

19. Additional Notices for Non-EU Users

Users and call recipients located outside the EU/EEA may have data protection rights under their local law that differ from, or are in addition to, the rights described in Section 18. We will honor applicable local rights upon verified request, to the extent required by law.

Users placing calls to or from jurisdictions with specific call-recording consent requirements (see Section 8.1 and Annex A) remain responsible for compliance with those requirements, regardless of where Ostora Group or its infrastructure is located.

19.1 Notice for California Residents

Residents of California whose personal data is processed in connection with the Service may have rights under the California Consumer Privacy Act, as amended ("CCPA"), including the right to know the categories of personal data collected, the right to request deletion, and the right to opt out of the sale or sharing of personal data. Ostora Group does not sell personal data as that term is defined under the CCPA. Requests under the CCPA may be submitted using the same process described in Section 18.1.

19.2 Notice for Pakistan-Based Users

Users and Team Members located in Pakistan should be aware that call and message monitoring described in this Policy is carried out consistent with the fraud-prevention rationale set out in Section 7, and that applicable Pakistani telecommunications and data protection law may impose additional obligations on the User or Administrator when placing calls to or from Pakistan, which remain the User's responsibility to observe.

20. Children's Privacy

The Service is a business-to-business platform intended for use by individuals who are at least 18 years of age, in a professional or commercial capacity. We do not knowingly collect personal data from children. If we become aware that we have inadvertently collected personal data from a child, we will take steps to delete such data promptly.

21. Third-Party Links and Services

The Service may contain links to, or integrations with, third-party websites, applications, or services that are not operated by Ostora Group, including but not limited to payment processors, telecommunications carriers, and productivity tools such as Google Sheets. This Policy does not apply to such third-party services, and we encourage you to review their respective privacy policies.

22. Changes to This Policy

We may update this Policy from time to time to reflect changes in our practices, the Service, or applicable law. Where changes are material, we will provide notice through the Service, by email, or by other reasonable means, prior to the changes taking effect. The "Last updated" / "Version" indication on the cover page of this document indicates when this Policy was last revised. Continued use of the Service after changes take effect constitutes acceptance of the revised Policy.

23. Governing Law and Jurisdiction

This Policy, and any dispute arising out of or in connection with it, shall be governed by the laws of Belgium, without regard to conflict-of-laws principles, without prejudice to any mandatory data protection rights you may have under the GDPR or the law of your habitual residence. The courts of Antwerp, Belgium shall have exclusive jurisdiction over any dispute arising from this Policy, save where mandatory consumer or data protection law provides otherwise.

24. Contact Us

For questions about this Policy, to exercise your data protection rights, or to report a suspected data security incident, please contact:

Ostora Group BV

Lange van Bloerstraat 51, 2060 Antwerpen, Belgium

Email: info@ostora.be

Website: ostnyx.com

Attn: Muneeb ur Rehman, Chairman / Haseeb Ali, Chief Executive Officer

24.1 Supervisory Authority

If you believe your data protection rights have not been respected, you have the right to lodge a complaint with the Belgian Data Protection Authority:

Gegevensbeschermingsautoriteit / Autorité de protection des données

Rue de la Presse 35, 1000 Brussels, Belgium

contact@apd-gba.be · www.autoriteprotectiondonnees.be

Annex A — Illustrative Call-Recording Consent Requirements by Jurisdiction

The following table is a non-exhaustive, illustrative summary provided for general reference only. It is not legal advice and must be verified against current local law before reliance. Requirements described as "all-party consent" generally require notice or consent from every participant on a call before recording; "one-party consent" jurisdictions generally permit recording with the consent of only one participant, which may be the User.

Jurisdiction	General Consent Standard
Belgium / EU (general)	Recording generally requires a valid GDPR legal basis and, in most contexts, prior notice to participants
Germany	Recording without the consent of all participants may constitute a criminal offense; consent generally required
France	Prior information/consent generally required under national data protection law
Netherlands	One-party consent is a recognized legal basis, though business notice is still commonly provided as best practice
United Kingdom	Notice generally required; recording permitted for legitimate business purposes under applicable data protection law
California, USA	All-party consent
Florida, USA	All-party consent
Illinois, USA	All-party consent
Pennsylvania, USA	All-party consent
Washington, USA	All-party consent
New York, USA	One-party consent
Texas, USA	One-party consent
Most other U.S. states	One-party consent (verify per state)
Canada (federal)	One-party consent, subject to provincial variation
Australia	Consent requirements vary by state/territory; verify applicable state surveillance-devices legislation
Pakistan	Notice/consent expectations should be confirmed against current local telecommunications and privacy law

Users placing or receiving calls in any jurisdiction not listed above should independently confirm applicable consent requirements before recording. This Annex will be reviewed and updated periodically but should not be treated as a substitute for current legal advice.

Annex B — Illustrative Fraud and Abuse Indicators Monitored

As part of the fraud-prevention and platform-integrity monitoring described in Section 7, Ostora Group monitors for indicators including, but not limited to, those set out below. This list is illustrative, non-exhaustive, and maintained internally in greater operational detail; it is disclosed here in summary form for transparency.

Indicator Category	Example
Abnormal calling volume	A single account placing an unusually high number of calls in a short period, inconsistent with normal use
Repeated short-duration calls	Patterns consistent with number-scanning or robocalling rather than genuine conversations
High complaint or block rate	A disproportionate number of call recipients blocking, reporting, or flagging a number as spam
Payment anomalies	Use of stolen or high-risk payment methods, rapid wallet top-ups followed by high-volume calling
Caller ID manipulation	Attempts to spoof or misrepresent the origin of a call outside normal caller-ID configuration
Content-based indicators	Recorded or transcribed content consistent with known scam scripts, upon review triggered by another indicator

Detection of one or more indicators does not automatically result in account suspension; flagged accounts are subject to human review consistent with Section 9.1 before any restrictive action is taken, except where immediate suspension is necessary to prevent ongoing harm.

Annex C — Sub-Processor Register

The following register identifies the categories of sub-processors currently engaged by Ostora Group in connection with the Service. Specific vendor names and locations are maintained in Ostora Group's internal vendor records and will be made available to organizational customers upon reasonable request, consistent with any applicable Data Processing Agreement.

Category	Function	Data Categories Involved
Telecommunications carrier(s)	Voice call routing, SMS delivery, number provisioning	Call metadata, call recordings (in transit), message content, phone numbers
Call-routing infrastructure provider	Bridging calls between Users and destination numbers	Call metadata, call recordings (in transit)
Payment processor	Processing card and wallet payments	Billing name/address, payment method tokens
Cloud hosting and database provider	Storage and hosting of application data	All categories described in Section 5

Ostora Group maintains, or is in the process of finalizing, signed Data Processing Agreements with each sub-processor identified above, consistent with Article 28 of the GDPR. Organizational customers with a separate Data Processing Agreement with Ostora Group will be notified of any intended change to this sub-processor register in accordance with the terms of that agreement.

Document Control

Field	Detail
Document title	Ostnyx Privacy Policy
Owner	Ostora Group BV
Prepared for	Muneeb ur Rehman, Chairman; Haseeb Ali, Chief Executive Officer
Version	1.0
Status	Draft — pending legal review
Effective date	1 August 2026

This document was prepared as a working draft to support Ostora Group's compliance efforts. It should be reviewed by qualified Belgian/EU data protection counsel, and by counsel familiar with the call-recording consent laws of each jurisdiction in which Ostnyx operates, before publication. Bracketed placeholders (retention periods, effective date, and specific vendor identities in Annex B) must be finalized, and all factual statements — including the existence of signed Data Processing Agreements with each sub-processor — should be confirmed as accurate before this Policy is published.