Privacy Notice

Version: 1.0
Effective date: *June 1, 2026*

This Privacy Notice explains how the operator of the website available at **https://nova-sms.com**, acting under the commercial brand **NOVA SMS** ("**NOVA SMS**", "**we**", "**us**" or "**our**"), processes personal data when you access or use the website, dashboard, application programming interface, virtual number functionality, SMS activation functionality, support channels, and any related services, features, content, or tools (collectively, the "**Services**").

Capitalized terms not defined in this Privacy Notice have the meanings given to them in the applicable Terms of Service or other service terms made available through the Services.

By using the Services, you acknowledge that you have read and understood this Privacy Notice.

1. Who we are

NOVA SMS is the commercial brand under which the Services are made available. For purposes of this Privacy Notice, NOVA SMS acts as the controller of personal data processed in connection with the operation, administration, security, support, and improvement of the Services.

NOVA SMS operates through a combination of internal resources, affiliated service arrangements, contractors, processors, infrastructure providers, technical partners, payment providers, fraud prevention providers, analytics providers, customer support tools, and other service providers as necessary to make the Services available.

NOVA SMS may provide the Services internationally and may rely on service providers, infrastructure providers, or upstream number providers located in multiple jurisdictions.

For privacy-related questions, requests, or notices, you may contact us at:

- **Email: contact@nova-sms.com**

2. Scope of this Privacy Notice

This Privacy Notice applies to personal data that we process in connection with:

- visits to our website and landing pages;
- account registration, login, and account administration;
- purchases, balance top-ups, billing, invoicing, and payment verification;
- use of virtual numbers, SMS activation workflows, API calls, and related technical operations;
- customer support communications and dispute handling;
- fraud detection, abuse prevention, platform security, and legal compliance; and
- analytics, diagnostics, service maintenance, and improvement.

This Privacy Notice does not apply to third-party websites, platforms, payment interfaces, or services that are not controlled by NOVA SMS, even if linked from or used together with the Services. Those third parties may process personal data under their own privacy notices and terms.

3. Categories of personal data we process

Depending on how you use the Services, we may process the following categories of personal data:

3.1 Account and profile data

We may process:

- email address;
- username or account identifier;
- password hash and authentication credentials;
- country or region, if provided or inferred for compliance or localization purposes;
- account status, risk flags, verification status, and internal account notes; and
- any profile information or settings you choose to submit.

3.2 Transaction and payment data

We may process:

- payment status and payment method metadata;
- transaction identifiers;
- billing records, top-up amounts, timestamps, and currency information;
- anti-fraud signals associated with payments;
- chargeback, refund, and dispute records; and
- limited payment-related information made available to us by payment processors.

NOVA SMS does not store full payment card numbers unless expressly stated otherwise. Card payments, wallet payments, bank transfers, and other payment operations may be handled by independent payment service providers.

3.3 Service usage and technical data

We may process:

- IP address;
- device and browser metadata;
- operating system and language settings;

- log files, access timestamps, session events, and API request metadata;
- referral URLs, clickstream data, and interaction data;
- account activity records;
- selected service, selected country, selected platform, order metadata, and number allocation metadata; and
- diagnostic and security event information.

3.4 Communications and support data

We may process:

- the content of messages sent to support;
- attachments or screenshots you provide;
- records of complaints, disputes, or enforcement actions; and
- correspondence concerning legal requests, abuse reports, refunds, or account issues.

3.5 SMS-related operational data

In connection with virtual number and SMS activation workflows, we may process:

- allocated temporary numbers or number identifiers;
- provider identifiers;
- timestamps relating to number allocation and message receipt;
- destination service or platform selected by the user;
- delivery status and technical routing information; and
- the content of incoming messages to the extent technically necessary to display, relay, troubleshoot, secure, or investigate the requested service.

Unless a longer retention period is required for security, fraud prevention, dispute handling, chargeback investigation, legal compliance, or enforcement of our Terms, message content is intended to be processed on a temporary, limited-access basis and may be discarded after the relevant session, display, or operational purpose has been completed.

4. Sources of personal data

We may obtain personal data:

- directly from you;
- automatically from your device or browser when you use the Services;

- from payment processors and anti-fraud providers;
- from analytics, hosting, infrastructure, and security providers;
- from upstream number providers and technical suppliers involved in delivering the Services;
- from customer support tools and communication channels; and
- from law enforcement agencies, regulators, courts, or other third parties where legally required or reasonably necessary.

5. Purposes of processing

We process personal data for the following purposes:

- to provide, operate, maintain, and administer the Services;
- to register and authenticate accounts;
- to allocate numbers, receive messages, and technically perform SMS activation workflows;
- to process purchases, top-ups, refunds, payment checks, and transaction administration;
- to communicate with users regarding service operations, support, incidents, or updates;
- to detect, prevent, investigate, and address fraud, abuse, unauthorized use, suspicious activity, money laundering risk, sanctions risk, chargebacks, and other harmful or unlawful conduct;
- to monitor reliability, performance, and security of the Services;
- to enforce the Terms of Service and other policies;
- to comply with legal, regulatory, accounting, tax, and law enforcement obligations;
- to establish, exercise, or defend legal claims; and
- to analyze usage trends and improve the functionality, usability, and security of the Services.

6. Legal bases for processing

To the extent applicable under relevant data protection law, we rely on one or more of the following legal bases:

- performance of a contract or steps taken at your request before entering into a contract;
- compliance with legal obligations;
- our legitimate interests in operating, securing, supporting, improving, and enforcing the Services, provided those interests are not overridden by applicable law;
- prevention of fraud, abuse, unauthorized access, and illegal activity;

- protection of our rights, property, users, providers, and business operations; and
- your consent, where consent is specifically required by applicable law.

Where we rely on consent, you may withdraw it at any time, but that will not affect the lawfulness of processing carried out before withdrawal.

7. Cookies and similar technologies

We may use cookies, SDKs, local storage, server logs, pixels, and similar technologies to:

- keep you logged in;
- remember preferences or settings;
- maintain session integrity;
- measure traffic and performance;
- detect abuse and suspicious activity; and
- improve functionality and user experience.

Some of these technologies are necessary for the operation and security of the Services. Others may be optional depending on the jurisdiction and configuration of the Services. Where required by law, we will request consent before using non-essential technologies.

You may control cookies through your browser or device settings, but disabling certain technologies may affect functionality.

8. Disclosure of personal data

We do not sell personal data in exchange for monetary consideration. We may disclose personal data only as reasonably necessary for the purposes described in this Privacy Notice, including to:

- hosting, cloud, infrastructure, and content delivery providers;
- payment processors, payment gateways, fraud prevention providers, and financial partners;
- customer support and communications platform providers;
- analytics, monitoring, and security service providers;
- upstream number providers, telecom-related suppliers, routing partners, and technical vendors involved in making the requested functionality available;
- professional advisers, auditors, insurers, and legal counsel;
- courts, regulators, public authorities, law enforcement agencies, or other third parties where required by law or where reasonably necessary to protect rights, safety, or the integrity of the Services; and

- acquirers, investors, lenders, or counterparties in connection with an actual or proposed merger, acquisition, financing, reorganization, sale of assets, or similar corporate transaction, subject to appropriate confidentiality measures where applicable.

All such disclosures may involve recipients in multiple jurisdictions.

9. International transfers

Personal data may be transferred to, stored in, or accessed from countries outside the jurisdiction in which you are located, including where our providers, infrastructure, technical partners, or operational resources are located, to the extent necessary for the provision, administration, security, support, and improvement of the Services.

Where applicable law requires specific safeguards for international transfers, we will take commercially reasonable steps to implement appropriate transfer mechanisms or protective measures as required by that law.

10. Data retention

We retain personal data for as long as reasonably necessary for the purposes described in this Privacy Notice, including to provide the Services, maintain account records, complete transactions, prevent fraud, resolve disputes, respond to claims, comply with legal obligations, and enforce our agreements.

Retention periods may vary depending on the category of data, the sensitivity of the information, the purpose of processing, the existence of complaints or investigations, applicable limitation periods, and legal or regulatory requirements.

Without limiting the generality of the foregoing:

- account and transaction records may be retained for the duration of the account relationship and for up to 5 years afterward, unless a longer period is required or justified by law, tax, accounting, fraud prevention, or dispute resolution needs;

- technical logs, access logs, API logs, and security records may be retained for 12 to 24 months, and longer where reasonably necessary for investigations, abuse prevention, incident response, or legal compliance;

- support tickets, user communications, and dispute records may be retained for up to 24 months after closure of the relevant matter, and longer where reasonably necessary to establish, exercise, or defend legal claims;

- payment, refund, chargeback, and anti-fraud records may be retained for up to 5 years or longer where required by payment providers, financial counterparties, or applicable law; and

- SMS-related content may be retained on a temporary and limited-access basis for the duration of the relevant session and for a short additional period reasonably necessary for technical processing, troubleshooting, fraud prevention, abuse review, chargeback investigation, or legal compliance, after which it may be deleted or irreversibly discarded unless longer retention is required for a specific legitimate or legal reason.

We may also retain data in aggregated or de-identified form where permitted by applicable law.

11. Data security

We implement commercially reasonable technical, organizational, and administrative measures designed to protect personal data against unauthorized access, accidental loss, unlawful destruction, misuse, alteration, or disclosure.

These measures may include access controls, role-based restrictions, logging, provider due diligence, system monitoring, environment segregation, encrypted transmission where appropriate, and other security practices considered reasonable in light of the nature of the Services and the risks involved.

However, no method of transmission over the Internet or electronic storage is completely secure. Accordingly, NOVA SMS cannot guarantee absolute security and will not be liable for unauthorized access, loss, corruption, or disclosure except to the extent required by applicable law.

Users are responsible for maintaining the confidentiality of account credentials, securing their own devices and networks, and notifying us promptly of any suspected unauthorized use of their account.

12. Your rights

Depending on the law applicable to you, you may have the right to request access to personal data, correction of inaccurate data, deletion, restriction of processing, objection to certain processing, withdrawal of consent where processing is based on consent, portability, or the submission of a complaint to a competent supervisory authority.

These rights are not absolute and may be subject to legal exceptions, identity verification, technical feasibility, disproportionate effort, protection of the rights of others, recordkeeping obligations, fraud prevention needs, legal privilege, or other lawful limitations.

To exercise any applicable rights, contact us using the details listed in Section 1.

13. How we handle privacy requests

When we receive a privacy request, we may ask for information necessary to verify identity, confirm authority, clarify the scope of the request, and protect the privacy and security of other users.

We may deny or limit a request to the extent permitted by applicable law, including where the request is manifestly unfounded, excessive, repetitive, technically impracticable, would adversely affect the rights of others, would interfere with fraud prevention or security controls, or cannot be fulfilled due to legal obligations that require continued retention.

If we cannot fully comply with a request, we will generally explain the basis for that outcome to the extent legally permitted.

14. Automated processing and fraud controls

We may use automated tools, rules-based systems, and internal scoring mechanisms to detect abuse, suspicious activity, payment anomalies, account takeovers, spam patterns, sanctions concerns, excessive failed attempts, and other activity that may threaten the Services, users, providers, or third parties.

These tools may contribute to decisions such as transaction review, temporary delays, additional verification, service restrictions, account limitations, or account suspension where reasonably necessary to protect the platform and comply with legal or operational requirements.

Where applicable law grants rights related to automated decision-making, users may contact us to request review, express a point of view, or contest a decision, subject to legal and operational limitations.

15. Children

The Services are not directed to children and are not intended for use by anyone under the age of 18 or any higher minimum age required under applicable law. We do not knowingly collect personal data directly from children.

If you believe that a child has provided personal data through the Services, contact us and we will take appropriate steps to investigate and, where appropriate, delete the data.

16. Nature of the Services

NOVA SMS does not represent itself as a public telecommunications operator unless expressly stated otherwise. NOVA SMS acts solely as a technical platform facilitating access to temporary numbers, message receipt functionality, API connectivity, and related technical services made available through upstream providers, infrastructure partners, and service suppliers.

This Privacy Notice applies to NOVA SMS's processing activities in connection with that technical platform role.

17. Third-party services

The Services may interface with or depend on third-party websites, payment systems, APIs, software, infrastructure, and external platforms. We are not responsible for the privacy practices of third parties that operate independently from NOVA SMS.

Users should review the privacy notices and terms of those third parties before interacting with them.

18. Changes to this Privacy Notice

We may amend or update this Privacy Notice at any time by posting a revised version on the website or otherwise making it available through the Services.

Unless applicable law requires a different approach, the revised version becomes effective on the effective date stated in the updated notice. Your continued use of the Services after the updated Privacy Notice becomes effective constitutes acceptance of the revised notice.

19. Language and interpretation

This Privacy Notice may be made available in more than one language. In the event of any inconsistency, ambiguity, or conflict between versions, the English version will prevail unless mandatory law requires otherwise.

Headings are for convenience only and do not affect interpretation.

20. Contact

For any privacy-related request, complaint, inquiry, or notice, contact:

NOVA SMS Privacy Contact
Email: **contact@nova-sms.com**

Website: **https://nova-sms.com**

By using the Services, you acknowledge that personal data may be processed as described in this Privacy Notice.