Nyzer Privacy Policy

Last Updated: November 12, 2025

Effective Date: November 12, 2025

Version: 2.0

Introduction

This Privacy Policy describes how Chronology Enterprises S.R.L. ("Nyzer," "we," "us," or "our") collects, uses, discloses, and protects your information when you use the Nyzer mobile application, website, and related services (collectively, the "Service").

We are committed to protecting your privacy and ensuring transparency about our data practices. By using the Service, you agree to the collection and use of information in accordance with this Privacy Policy.

Company Information:

Chronology Enterprises S.R.L.

Av. Ortega Y Gasset #16

Ensanche la Fe, D.N. Santo Domingo

10514, República Dominicana

Email: contact@nyzerapp.com

Phone: +1 849-868-1908

Website: https://www.nyzerapp.com

Table of Contents

1. Information We Collect

We collect information that you provide directly to us, information we obtain automatically when you use our Service, and information from third-party sources.

1.1 Personal Information You Provide

Account Information:

Name (first and last)

Email address

Phone number

Password (encrypted)

Date of birth (for age verification)

Profile Information:

Profile picture (optional)

User preferences and settings

Service preferences

Gender (optional)

Transaction Information:

Last 4 digits of payment card (for transaction identification only)

Transaction history

Booking details

Payment amounts

Transaction dates and times

Payment identifiers

SMB (service provider) information related to your bookings

Communication Data:

Messages sent through our in-app chat system

Voice notes sent through in-app chat (stored up to 1 year or until deleted by user)

Customer support communications

Reviews and ratings you provide

User-Generated Content:

Photos uploaded to your profile

Photos of services (for SMBs)

Photos attached to reviews

Other content you choose to share through the Service

1.2 Information Collected Automatically

Device Information:

Device model and manufacturer

Operating system and version

Unique device identifiers (Device ID)

Mobile network information

IP address

Browser type and version (website only)

Usage Information:

App screens visited

Features used

Time spent in app

Session duration

Search queries

Interaction with SMB profiles

Booking patterns

App performance data

Location Information (Optional):

Coarse location (city/region) - collected only when you search for nearby services

Location permissions are completely optional; the app functions fully without location access

You can revoke location permissions at any time through your device settings

Analytics Data:

App usage patterns

Feature adoption metrics

Performance metrics

Error logs and crash reports

A/B test assignments (to improve app features)

1.3 Information from Third-Party Sources

Social Media Login Data:

When you choose to sign in using a third-party service, we collect:

Google Sign-In: Profile information (name, email address, profile picture)

Apple Sign-In: Name, email address (real or private relay), and user identifier

Facebook Sign-In (Future): Profile information as permitted by your Facebook privacy settings

We do NOT collect:

Your social media contacts

Your social media posts or activity

Any data beyond basic profile information necessary for account creation

2. How We Use Your Information

We process your personal information only for the purposes described below and only when we have a legal basis to do so.

2.1 Service Delivery (Legal Basis: Contract Performance)

Create and manage your account

Process and facilitate bookings with service providers (SMBs)

Process payments and transactions

Send transactional communications (booking confirmations, appointment reminders, receipts)

Provide customer support

Facilitate communication between customers and SMBs

Display your profile to SMBs when you book services

2.2 Service Improvement (Legal Basis: Legitimate Interest)

Analyze app usage to improve features and functionality

Conduct A/B testing to optimize user experience

Monitor app performance and fix technical issues

Develop new features and services

Understand user preferences and behavior patterns

2.3 Security and Fraud Prevention (Legal Basis: Legitimate Interest & Legal Obligation)

Detect and prevent fraudulent bookings and transactions

Verify user identity and age

Monitor for violations of our Terms of Use

Protect against unauthorized access or use

Investigate suspected violations

Maintain security logs and access records

2.4 Legal Compliance (Legal Basis: Legal Obligation)

Comply with applicable laws and regulations

Respond to legal requests from authorities

Enforce our Terms of Use

Maintain transaction records for tax purposes (up to 7 years)

Comply with payment processing regulations (PCI DSS)

2.5 Communications (Legal Basis: Contract Performance)

We send ONLY transactional communications:

Booking confirmations

Appointment reminders

Payment receipts

Account security notifications

Service updates that affect your bookings

Responses to your inquiries

We do NOT send:

Marketing emails

Promotional SMS messages

Unsolicited newsletters

Advertising communications

Note: You can manage communication preferences in your app settings. Standard SMS and data rates may apply.

3. How We Share Your Information

We do not sell, rent, or trade your personal information to third parties for marketing purposes. We share your information only in the following limited circumstances:

3.1 With Service Providers (SMBs)

When you book an appointment, the SMB receives:

Your full name

Confirmation that payment has been processed

Last 4 digits of your payment card (for in-store validation if necessary)

Your appointment history with that specific SMB (retained by SMB for up to 1 year)

SMBs do NOT receive:

Your full payment card information

Your email address (unless you share it directly)

Your phone number (unless you share it directly)

Your personal data from other bookings with different SMBs

Important: SMBs are independent data controllers responsible for safeguarding your information and must comply with applicable data protection laws.

3.2 With Third-Party Service Providers

We share limited data with trusted third-party providers who help us deliver our Service:

Payment Processing:

Azul: Processes payment transactions securely. We do NOT store your full payment card information. Azul is PCI DSS Level 1 compliant.

Email Services:

Amazon SES: Sends transactional emails (booking confirmations, receipts, password resets).

Search Functionality:

Typesense: Processes search queries only (search input text) to provide fast search results.

Infrastructure and Hosting:

Firebase / Google Cloud Platform (GCP): Hosts application data, user accounts, photos, and provides security features. Data is stored in GCP's multi-region configuration.

Analytics:

Firebase Analytics: Collects anonymized usage data to improve app functionality.

Google Analytics: Collects website and mobile app usage data (linked to user account for personalization purposes).

Authentication:

Firebase Authentication: Manages user login and account security.

Google Sign-In SDK: Facilitates sign-in with Google accounts.

Apple Sign-In: Facilitates sign-in with Apple ID.

All third-party providers:

Are contractually obligated to protect your data

May only use your data to provide services to Nyzer

Must comply with applicable privacy laws

Are prohibited from selling or using your data for their own purposes

3.3 For Legal Reasons

We may disclose your information if required by law or in good faith belief that such action is necessary to:

Comply with legal obligations, court orders, or government requests

Enforce our Terms of Use and other agreements

Protect our rights, property, or safety

Protect the rights, property, or safety of our users or the public

Prevent fraud or security threats

3.4 Business Transfers

If Nyzer is involved in a merger, acquisition, sale of assets, or bankruptcy, your information may be transferred as part of that transaction. We will notify you via email and/or prominent notice in the app at least 30 days before any such transfer and provide information about your choices.

3.5 With Your Consent

We may share your information for other purposes with your explicit consent.

4. Data Retention

We retain your personal information only as long as necessary to fulfill the purposes described in this Privacy Policy, or as required by law.

4.1 Active Account Data

While your account is active:

Profile information: Retained indefinitely until you delete it or your account

Appointment history: Retained for up to 1 year

Chat messages: Retained for up to 1 year (you can delete messages at any time)

Voice notes: Retained for up to 1 year (you can delete at any time)

Search history: Retained for up to 1 year

Profile photos: Retained indefinitely until you remove them or delete your account

Reviews: Retained indefinitely or until you delete them

4.2 Deleted Account Data

When you delete your account:

Immediately Deleted (within 5 business days):

Profile information (name, email, phone, password)

Appointment history (non-transaction details)

Payment methods and last 4 digits

Photos uploaded (profile pictures, review photos, service photos)

Chat messages and voice notes

Search history

User preferences and settings

Retained for Legal/Regulatory Purposes:

Transaction records (7 years): Required by tax laws. Includes:

Customer name

Customer email

Customer phone number

SMB name

Service details

Payment amount

Last 4 digits of card

Transaction date and time

Transaction ID

Payment identifier

Fraud prevention data (up to 24 months): Device IDs, IP addresses, and behavioral patterns used to prevent fraudulent activity

Backup copies (up to 1 year): Your deleted account data will be removed from backup systems within the next backup cycle, typically within 30-90 days, but no later than 1 year

Note: After 7 years, transaction records are automatically deleted unless retention is required by additional laws or government order.

4.3 Anonymized Data

We may retain anonymized or aggregated data that cannot identify you personally for analytical purposes indefinitely.

5. Your Privacy Rights

You have the following rights regarding your personal information:

5.1 Access and Portability

Right to Access: You can request a copy of all personal data we hold about you.

How to Request:

Email: contact@nyzerapp.com

Response time: 5 business days

Format: Exportable file (JSON/PDF)

Right to Data Portability: You can receive your data in a structured, machine-readable format to transfer to another service.

5.2 Correction

Right to Rectification: You can update or correct inaccurate personal information.

How to Correct:

Via in-app profile settings (immediate)

Email: contact@nyzerapp.com (5 business days)

5.3 Deletion

Right to Erasure: You can request deletion of your account and personal data.

How to Delete:

Mobile App: Account deletion is immediate via app settings

Website/Email: Deletion completed within 5 business days after security verification to prevent unauthorized deletion

Important Notes:

Deletion is irreversible

Some data must be retained for legal compliance (see Section 4.2)

You can request verification of deletion status after 30 days

5.4 Restriction and Objection

Right to Restrict Processing: You can request that we limit how we use your data in certain circumstances.

Right to Object: You can object to:

Processing based on legitimate interests

Use of your data for analytics (email contact@nyzerapp.com to opt out)

5.5 Withdraw Consent

You can withdraw previously granted consent at any time:

Location access: Revoke via device settings

Camera access: Revoke via device settings

Photo library access: Revoke via device settings

Microphone access: Revoke via device settings

Push notifications: Disable in app settings or device settings

SMS communications: Text STOP to +1 849-868-1908

5.6 Lodge a Complaint

If you believe we have violated your privacy rights, you have the right to file a complaint with:

Your local data protection authority (for EU residents)

The California Attorney General (for California residents)

Contact us directly at contact@nyzerapp.com

5.7 How to Exercise Your Rights

Contact us at:

Email: contact@nyzerapp.com

Phone: +1 849-868-1908

Mail: Chronology Enterprises S.R.L., Av. Ortega Y Gasset #16, Ensanche la Fe, D.N. Santo Domingo, 10514, República Dominicana

We will:

Respond within 5 business days

Verify your identity for security purposes (may require government-issued ID)

Provide requested information or take requested action within 30 days (may extend to 45 days for complex requests with notice)

6. Children's Privacy

6.1 Age Requirements

Nyzer is intended for users aged 13 and older. Users under 18 must have parental or guardian consent to use the Service.

Three ways minors (ages 13-17) can use Nyzer:

Option A - Parent-Created Account:

A parent or legal guardian creates and manages the account on behalf of the minor using the parent's email address and verification.

Option B - Parent-Approved Account:

The minor creates the account, but a parent or legal guardian must approve it via email verification and consent form.

Option C - Parental Consent:

The minor creates the account with parental consent as acknowledged in the Terms of Use. Parents are responsible for supervising their child's use of the Service.

6.2 Age Verification

We implement the following age verification measures:

Date of birth collection during registration

Automated flagging of accounts indicating users under 13

Manual review of suspected underage accounts

Identity verification when age is questioned

6.3 Underage Account Discovery

If we discover a user is under 13:

1. Account Suspension: The account is immediately suspended

2. Verification Request: We request proof of age or parental consent

3. Data Hold: All personal data is placed on hold (not deleted immediately)

4. 90-Day Period: If verification is not provided within 90 days:

The account is permanently deleted

All associated personal data is deleted within 5 business days

5. Successful Verification: If proper age verification or parental consent is provided, the account is reactivated

6.4 Parental Rights

Parents or legal guardians of users under 18 may:

Request access to their child's personal information

Request correction or deletion of their child's data

Refuse to allow further collection of their child's information

Withdraw consent for their child's use of the Service

To exercise parental rights, contact: contact@nyzerapp.com with proof of parental relationship.

6.5 Notice to Parents

We encourage parents to:

Monitor their children's online activities

Review this Privacy Policy with their children

Supervise their children's use of the Service

Contact us immediately if they believe their child has provided information without consent

7. Data Security

We implement industry-standard security measures to protect your personal information from unauthorized access, disclosure, alteration, or destruction.

7.1 Encryption

Data in Transit:

All data transmitted between your device and our servers is encrypted using TLS 1.2 or higher

HTTPS is enforced for all website communications

Data at Rest:

All personal data stored on our servers is encrypted using AES-256 encryption

Encryption keys are securely managed and rotated regularly

7.2 Payment Security

PCI DSS Compliance: Our payment processor (Azul) is PCI DSS Level 1 certified

No Card Storage: We do NOT store full payment card information, CVV/CVC codes, or PINs

Tokenization: Payment information is tokenized for secure processing

Last 4 Digits Only: We store only the last 4 digits of your card for transaction identification

7.3 Access Controls

Employee Access:

Access to personal data is restricted on a need-to-know basis

Role-based access control (RBAC) limits data access by job function

All access is logged and monitored

Employees sign confidentiality agreements

Background checks are conducted for employees with data access

Access Logging:

Every access to user accounts is logged with timestamp and employee ID

Access logs are reviewed monthly by supervisors

Suspicious access patterns trigger immediate investigation

7.4 Infrastructure Security

Firebase/GCP Security Features:

Multi-region redundancy for data availability

Automated security patches and updates

Network intrusion detection systems

DDoS protection

Regular security audits by Google Cloud Platform

Additional Measures:

Automated malware scanning

Regular vulnerability assessments

Penetration testing (annual)

Security awareness training for all employees

7.5 Security Certifications

We maintain the following security certifications and compliance standards:

SOC 2 Type II - Independent audit of security controls

ISO 27001 - Information security management system certification

PCI DSS - Payment Card Industry Data Security Standard (through our payment processor)

7.6 Your Security Responsibilities

To help protect your account:

Use a strong, unique password

Never share your password with others

Log out after each session on shared devices

Enable device security features (PIN, biometric authentication)

Report suspicious activity immediately to contact@nyzerapp.com

Keep your app updated to the latest version

7.7 Limitations

No Security System is 100% Secure:

Despite our security measures, no method of transmission over the internet or electronic storage is completely secure. While we strive to protect your personal information, we cannot guarantee absolute security.

You use the Service at your own risk and are responsible for maintaining the confidentiality of your account credentials.

8. International Data Transfers

8.1 Multi-Region Data Storage

Your personal information may be transferred to, stored, and processed in countries outside your country of residence, including the United States and other regions where our service providers (Firebase/Google Cloud Platform) maintain infrastructure.

GCP Multi-Region Configuration:

Our data is stored using Google Cloud Platform's multi-region configuration, which distributes data across multiple geographic locations for redundancy and performance. For specific details about GCP's current multi-region locations, please refer to: https://cloud.google.com/about/locations

8.2 Adequacy and Safeguards

When we transfer data internationally, we ensure adequate protection through:

For European Union Users:

Standard Contractual Clauses (SCCs): We use European Commission-approved Standard Contractual Clauses for data transfers from the EU to countries without adequacy decisions

GDPR Chapter V Compliance: All international transfers comply with GDPR requirements

Additional Safeguards: Technical and organizational measures to ensure data security

For All Users:

Contractual obligations with service providers to protect your data

Encryption of data in transit and at rest (AES-256, TLS 1.2+)

Regular security audits and compliance reviews

Adherence to applicable data protection laws in each jurisdiction

8.3 Your Rights Regarding International Transfers

You have the right to:

Request information about the safeguards we use for international transfers

Object to international transfers in certain circumstances

Receive a copy of the Standard Contractual Clauses we use

To request information or exercise these rights, contact: contact@nyzerapp.com

9. Cookies and Tracking Technologies

9.1 Website Cookies

Our website (www.nyzerapp.com) uses cookies to enhance your browsing experience. Our mobile application does NOT use traditional browser cookies.

Types of Cookies We Use on the Website:

Essential Cookies (Cannot be Disabled):

Session authentication cookies

Security and fraud prevention cookies

Core functionality cookies (e.g., language preferences)

Performance Cookies (Can be Disabled):

Google Analytics cookies (website traffic analysis)

Error tracking cookies

Page load time measurement

Preference Cookies:

Language selection

Display preferences

Notification preferences

We do NOT use:

Advertising cookies

Third-party marketing cookies

Cross-site tracking cookies

9.2 Mobile App Tracking Technologies

While our mobile app does not use traditional cookies, we use similar technologies:

Firebase Remote Config:

Stores user preferences locally on your device

Manages A/B test assignments to improve features

Data is tied to your user account

Used to personalize your app experience

Local Storage:

App settings and preferences stored locally on your device

Cache for faster app performance

Can be cleared by deleting the app or clearing app data

Analytics SDKs:

Firebase Analytics (tracks app usage patterns)

Google Analytics (tracks feature adoption and user behavior)

Data is linked to your user account for personalization

9.3 Cookie Controls

Website Cookie Controls:

Most web browsers accept cookies by default

You can disable cookies through your browser settings (Help menu)

Note: Disabling cookies may limit website functionality

Mobile App Controls:

Analytics tracking: Cannot be disabled but data is anonymized where possible

Local data storage: Clear by uninstalling app or clearing app data

To opt out of analytics: Email contact@nyzerapp.com

9.4 Do Not Track

Our website and app do not currently respond to "Do Not Track" (DNT) browser signals, as there is no industry standard for DNT compliance. However, we do not track you across third-party websites or apps for advertising purposes.

10. Third-Party Services

10.1 Complete List of Third-Party Services

We use the following third-party services to provide and improve our Service. Each has its own privacy policy governing how they handle data:

Service Provider	Purpose	Data Shared	Privacy Policy
Firebase / Google Cloud Platform	App hosting, database, authentication, analytics	Account data, usage data, device data	https://firebase.google.com/support/privacy
Azul	Payment processing	Transaction data, last 4 card digits	https://www.azul.com.do/privacidad
Amazon SES	Transactional emails	Email address, name, booking details	https://aws.amazon.com/privacy/
Typesense	Search functionality	Search queries only	https://typesense.org/privacy/
Google Sign-In	Third-party authentication	Google profile data (name, email, photo)	https://policies.google.com/privacy
Apple Sign-In	Third-party authentication	Apple ID data (name, email)	https://www.apple.com/legal/privacy/
Google Analytics	Usage analytics (web & mobile)	Usage patterns, device info	https://policies.google.com/privacy

10.2 Data Processing Agreements

All third-party service providers:

Have signed Data Processing Agreements (DPAs) or equivalent contracts

Are contractually prohibited from using your data for their own purposes

Must comply with applicable data protection laws (GDPR, CCPA, etc.)

Implement appropriate security measures

May only process data on our instructions

10.3 No Data Sales

We do NOT:

Sell your personal information to third parties

Rent or lease your data to data brokers

Share your data with advertisers

Use your data for third-party marketing

Track you across other apps or websites for advertising

10.4 Third-Party Links

Our Service may contain links to third-party websites or services that are not operated by us. We are not responsible for the privacy practices of these third parties. We encourage you to review the privacy policies of any third-party sites you visit.

10.5 Social Media Integration

Current Integration:

Google Sign-In (optional login method)

Apple Sign-In (optional login method)

Future Integration:

Facebook Sign-In (planned)

We do NOT:

Share your data with social media platforms except for basic authentication

Post to your social media accounts without permission

Import your social media contacts

Track your social media activity

User-Initiated Sharing:

Users can take screenshots and share them on social media

This is outside our control and not tracked by us

11. Automated Decision-Making

We use automated systems for certain decisions, but all significant decisions are subject to human review.

11.1 Automated Processes

The following processes are automated with human oversight:

Content Moderation:

Automated scanning of reviews, chat messages, and photos for violations of our Terms of Use

Flagging of potentially inappropriate content (hate speech, violence, illegal activity, explicit content)

Human Review: All flagged content is reviewed by a human moderator before final action

User Appeal: You can appeal content removal decisions to contact@nyzerapp.com

Fraud Detection:

Automated analysis of transaction patterns to detect fraudulent bookings

IP address monitoring, device fingerprinting, and behavioral analysis

Human Review: Suspicious transactions are reviewed by our fraud prevention team before account action

User Appeal: If your account is flagged, contact contact@nyzerapp.com with documentation

Payment Transaction Rejection:

Automated screening of payment transactions for security (performed by Azul)

High-risk transactions may be automatically declined

Human Review: You can contact customer support for manual review

User Appeal: Email contact@nyzerapp.com if you believe your transaction was wrongly rejected

Search Result Rankings:

Automated algorithm determines the order of SMBs in search results based on factors described in our Terms of Use (Section 4.10)

Factors include: location, availability, ratings, promotions, profile views-to-bookings ratio

Transparency: Rankings are based on objective criteria to provide relevant results

No Human Intervention: Search rankings are fully automated and not manually adjusted

Terms of Use Violations:

Automated detection of policy violations (spam, prohibited content, unauthorized business)

Account flagging for review

Human Review: All account suspensions or bans are reviewed by a human before final action

User Appeal: Appeal suspensions or bans to contact@nyzerapp.com

11.2 Your Rights Regarding Automated Decisions

You have the right to:

Request human review of any automated decision that affects you

Understand the logic and criteria used in automated decision-making

Challenge automated decisions and provide additional context

Appeal decisions via contact@nyzerapp.com

Response Time: We will respond to appeals within 5-7 business days.

11.3 No Profiling with Legal Effects

We do NOT use automated decision-making or profiling that produces legal effects or similarly significantly affects you without human intervention.

12. Data Breach Notification

We take data security seriously and have procedures in place to respond to any potential data breach.

12.1 Our Breach Response Process

In the event of a data breach affecting your personal information, we will:

1. Immediate Investigation (0-24 hours):

Assess the scope and nature of the breach

Identify affected users and types of data compromised

Contain the breach to prevent further unauthorized access

2. Containment and Remediation (24-72 hours):

Implement measures to stop the breach

Secure affected systems

Work with security experts and law enforcement if necessary

3. User Notification:

Timing: Within 72 hours of discovering the breach (GDPR requirement for EU users) or as required by applicable law for other jurisdictions

Method: Email to your registered email address, in-app notification, and public notice on www.nyzerapp.com

Information Provided:

Nature and scope of the breach

Types of personal data affected (e.g., names, emails, payment data)

Date of the breach

Steps we are taking to address the breach

Steps you can take to protect yourself (e.g., change passwords, monitor accounts)

Contact information for questions and support

4. Authority Notification:

We will notify relevant data protection authorities as required by law:

EU: Within 72 hours to the appropriate supervisory authority

California: As required by California Civil Code § 1798.82

Other jurisdictions: As required by applicable breach notification laws

12.2 Our Track Record

Data Breach History: We have never experienced a data breach or security incident involving unauthorized access to personal information.

We continuously monitor our systems and maintain robust security measures to prevent breaches.

12.3 What You Should Do

If you receive a data breach notification from us:

1. Read it carefully and understand what data was affected

2. Follow our recommended actions immediately

3. Change your password if advised

4. Monitor your accounts for suspicious activity

5. Contact us at contact@nyzerapp.com with any questions

Report Suspicious Activity:

If you suspect unauthorized access to your account, contact us immediately at contact@nyzerapp.com or +1 849-868-1908.

13. Changes to This Privacy Policy

13.1 Policy Updates

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors.

Types of Changes:

Material Changes (Affecting Your Rights):

Changes to the types of data we collect

New purposes for processing your data

Changes to data sharing practices

Reduction in data retention periods

Notice: 30 days advance notice via email and prominent in-app notification

Consent: Continued use of the Service after the 30-day notice period constitutes acceptance of the updated policy. For significant changes, we may require explicit consent before you can continue using the Service.

Minor Changes (Clarifications, Updates):

Corrections to contact information

Updates to third-party links

Clarifications of existing practices

Notice: Posted on www.nyzerapp.com with updated "Last Updated" date

Effective Immediately: Minor changes take effect upon posting

13.2 Version History

We maintain a version history of our Privacy Policy. Previous versions are available at:

https://www.nyzerapp.com/privacy-history

Current Version: 2.0

Effective Date: November 12, 2025

Last Updated: November 12, 2025

13.3 How You Will Be Notified

For Material Changes:

Email notification to your registered email address

Prominent in-app banner notification

Posted on our website homepage

For Minor Changes:

Updated "Last Updated" date at the top of this policy

Posted on our website

13.4 Review Responsibility

We encourage you to review this Privacy Policy periodically to stay informed about how we protect your information. You can always find the most current version at:

https://www.nyzerapp.com/legaldocs/PrivacyPolicy_Nyzer.pdf

14. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us:

General Privacy Inquiries:

Email: contact@nyzerapp.com

Phone: +1 849-868-1908

Response Time: Within 5 business days

Data Subject Access Requests:

Email: contact@nyzerapp.com

Subject Line: "Privacy Rights Request"

Expected Response: 5-30 business days (depending on complexity)

Mailing Address:

Chronology Enterprises S.R.L.

Attention: Privacy Officer

Av. Ortega Y Gasset #16

Ensanche la Fe, D.N. Santo Domingo

10514, República Dominicana

For Customer Support:

Email: help.us@nyzerapp.com (Customers)

Email: info.us@nyzerapp.com (SMBs/Service Providers)

For Security Issues:

Email: contact@nyzerapp.com

Subject Line: "URGENT: Security Issue"

We will respond to security reports within 24 hours.

15. Region-Specific Privacy Rights

Depending on your location, you may have additional privacy rights under local laws.

15.1 European Union (EU) / European Economic Area (EEA) Users - GDPR Rights

If you are located in the EU/EEA, you have additional rights under the General Data Protection Regulation (GDPR).

Legal Basis for Processing

We process your personal data based on the following legal grounds:

Contract Performance:

Service delivery (bookings, payments, account management)

Communication with you about your bookings

Providing customer support

Legitimate Interests:

Fraud prevention and security

Service improvement and analytics

Business operations and administration

Our legitimate interests are balanced against your rights and do not override your fundamental rights

Consent:

Location data collection (you can withdraw consent via device settings)

Camera and photo library access (you can withdraw consent via device settings)

Microphone access for voice notes (you can withdraw consent via device settings)

A/B testing and personalization features

Legal Obligation:

Tax record retention (7 years)

Compliance with payment processing regulations

Response to lawful requests from authorities

Your GDPR Rights

Right to Access (Article 15):

Request confirmation of whether we process your personal data

Receive a copy of your personal data

Request information about processing purposes, categories, and recipients

Right to Rectification (Article 16):

Correct inaccurate personal data

Complete incomplete personal data

Right to Erasure / "Right to be Forgotten" (Article 17):

Request deletion of your personal data when:

Data is no longer necessary for the original purpose

You withdraw consent

You object to processing

Data was unlawfully processed

Exceptions: We may retain data when required by legal obligations (tax records, fraud prevention)

Right to Restriction of Processing (Article 18):

Request limitation of processing when:

You contest the accuracy of data

Processing is unlawful but you don't want erasure

We no longer need the data but you need it for legal claims

You object to processing pending verification

Right to Data Portability (Article 20):

Receive your personal data in a structured, commonly used, machine-readable format

Transmit your data to another controller

Right to Object (Article 21):

Object to processing based on legitimate interests

Object to direct marketing (though we don't send marketing communications)

Object to automated decision-making and profiling

Right to Withdraw Consent (Article 7):

Withdraw consent at any time for processing based on consent

Withdrawal does not affect lawfulness of processing before withdrawal

Right to Lodge a Complaint (Article 77):

File a complaint with your local supervisory authority (data protection authority)

List of EU supervisory authorities: https://edpb.europa.eu/about-edpb/board/members_en

Data Controller Information

Data Controller: Chronology Enterprises S.R.L.

Note: We do not currently have a dedicated Data Protection Officer (DPO) or EU Representative as our processing volume does not require these roles under GDPR. If this changes, we will update this policy.

Contact for GDPR Requests:

Email: contact@nyzerapp.com

Subject: "GDPR Data Subject Request"

International Data Transfers from EU

Your data may be transferred to countries outside the EU/EEA. We ensure adequate protection through:

Standard Contractual Clauses (SCCs): EU Commission-approved clauses with service providers

Adequacy Decisions: Transfers to countries with EU adequacy decisions where applicable

Additional Safeguards: Technical and organizational security measures

To request a copy of the SCCs we use, contact: contact@nyzerapp.com

15.2 California Residents - CCPA/CPRA Rights

If you are a California resident, you have rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA).

Categories of Personal Information Collected

In the past 12 months, we have collected the following categories of personal information:

| Category | Examples | Collected? | Business Purpose |

|||||

| Identifiers | Name, email, phone, device ID, IP address | ✓ Yes | Account management, service delivery, fraud prevention |

| Commercial Information | Transaction history, booking details, payment amounts | ✓ Yes | Service delivery, tax compliance |

| Internet/Network Activity | App usage, search history, device info | ✓ Yes | Service improvement, analytics, security |

| Geolocation Data | Coarse location (city/region) | ✓ Yes | Service provider search (optional) |

| Audio/Electronic Data | Voice notes in chat | ✓ Yes | In-app communication |

| Visual Information | Profile photos, review photos | ✓ Yes | Profile display, reviews |

| Inferences | Service preferences, user behavior patterns | ✓ Yes | Personalization, service improvement |

| Sensitive Personal Information | N/A | ✗ No | We do not collect sensitive personal information as defined by CPRA |

Sources of Personal Information

Directly from you: Account registration, bookings, communications

Automatically collected: Device information, usage data, analytics

Third-party sources: Google Sign-In, Apple Sign-In (profile data only)

Business Purposes for Collection

Providing and managing the Service

Processing transactions and bookings

Fraud prevention and security

Legal compliance (tax records, regulatory requirements)

Service improvement and analytics

Customer support

Categories of Third Parties We Share With

Service providers: Firebase/GCP, Azul, Amazon SES, Typesense (for service delivery only)

SMBs: Limited information when you book appointments (name, payment confirmation)

Authorities: When required by law

Sale of Personal Information

WE DO NOT SELL YOUR PERSONAL INFORMATION.

We have not sold personal information in the past 12 months and do not plan to sell personal information in the future.

Your CCPA/CPRA Rights

Right to Know (§1798.100):

Request disclosure of:

Categories of personal information collected

Categories of sources

Business purpose for collection

Categories of third parties with whom we share information

Specific pieces of personal information collected about you

Right to Delete (§1798.105):

Request deletion of personal information we collected from you

Exceptions: We may retain information when necessary for:

Legal compliance (tax records - 7 years)

Fraud prevention (24 months)

Completing transactions

Security and debugging

Internal lawful uses

Right to Correct (§1798.106):

Request correction of inaccurate personal information

Right to Opt-Out of Sale/Sharing (§1798.120):

Not applicable - we do not sell or share personal information for cross-context behavioral advertising

Right to Limit Use of Sensitive Personal Information (§1798.121):

Not applicable - we do not collect or use sensitive personal information as defined by CPRA

Right to Non-Discrimination (§1798.125):

We will not discriminate against you for exercising your CCPA/CPRA rights

We will not:

Deny you services

Charge different prices or rates

Provide different quality of service

Suggest you will receive different pricing or quality

How to Exercise Your California Rights

Submit a Request:

Email: contact@nyzerapp.com with subject "CCPA Request"

Phone: +1 849-868-1908

Mail: Chronology Enterprises S.R.L., Attention: Privacy Rights Request, Av. Ortega Y Gasset #16, Ensanche la Fe, D.N. Santo Domingo, 10514, República Dominicana

Verification Process:

We will verify your identity to protect your information

May require: Government-issued ID, account verification questions, or two-step authentication

For deletion requests, we may require additional verification

Response Time:

We will respond within 45 days of receiving your request

May extend for an additional 45 days if needed (we will notify you)

Authorized Agents:

You may designate an authorized agent to make requests on your behalf

The agent must provide:

Written authorization signed by you

Proof of their identity

Verification that they are registered with the California Secretary of State (if applicable)

California Consumer Rights Notice

Under California Civil Code Section 1789.3, California users are entitled to the following consumer rights notice:

Complaint Assistance:

The Complaint Assistance Unit of the Division of Consumer Services of the California Department of Consumer Affairs may be contacted at:

Address:

1625 North Market Blvd., Suite N-112

Sacramento, CA 95834

Phone:

(916) 445-1254 or (800) 952-5210

Website:

https://www.dca.ca.gov

California "Shine the Light" Law

California Civil Code Section 1798.83 permits California residents to request information about disclosure of personal information to third parties for direct marketing purposes. We do not disclose personal information to third parties for their direct marketing purposes.

15.3 Other U.S. States

If you reside in other U.S. states with comprehensive privacy laws (e.g., Virginia, Colorado, Connecticut, Utah), you may have similar rights to California residents. Contact us at contact@nyzerapp.com to exercise your rights.

15.4 Dominican Republic Residents

As a Dominican company, we comply with Law No. 172-13 on Comprehensive Protection of Personal Data in the Dominican Republic.

Your Rights Under Law 172-13:

Right to access your personal data

Right to rectify inaccurate data

Right to cancel or delete your data

Right to object to processing

Right to revoke consent

Dominican Republic Data Protection Authority:

Contact information available at: https://www.indotel.gob.do

15.5 Other Jurisdictions

If you are located outside the EU, California, or Dominican Republic, you may have privacy rights under your local laws. Contact us at contact@nyzerapp.com to learn more about your rights.

16. App Store and Google Play Specific Disclosures

16.1 Apple App Store Privacy "Nutrition Label"

The following data types are collected and linked to your identity for the purposes indicated:

CONTACT INFORMATION

Name: App Functionality

Email Address: App Functionality

Phone Number: App Functionality (NOT used for advertising or marketing)

LOCATION

Coarse Location: App Functionality (optional, for finding nearby services)

IDENTIFIERS

User ID: App Functionality, Analytics

Device ID: App Functionality, Analytics

USAGE DATA

Other Usage Data: Analytics

DIAGNOSTICS

Other Diagnostic Data: Analytics (not linked to identity)

OTHER DATA

Other Data Types: App Functionality, Analytics

TRACKING: We do NOT track you across apps and websites owned by other companies for advertising or marketing purposes.

DATA LINKED TO YOU: All personal data collected is linked to your user account.

DATA NOT LINKED TO YOU: Diagnostic crash data and anonymous analytics.

16.2 Google Play Data Safety Disclosures

DATA COLLECTED:

✓ Personal info (name, email address, phone number)

✓ Financial info (last 4 digits of payment card, transaction history)

✓ Location (approximate location - optional)

✓ Photos and videos (user-uploaded profile pictures, review photos)

✓ Audio files (voice notes in chat)

✓ App activity (in-app searches, app interactions)

✓ Device or other IDs (device identifiers for analytics and security)

DATA SHARED WITH THIRD PARTIES:

✓ Payment processors (Azul) - for transaction processing only

✓ Email services (Amazon SES) - for transactional emails only

✓ Cloud infrastructure (Firebase/GCP) - for data hosting and security

✓ Search functionality (Typesense) - for search queries only

SECURITY PRACTICES:

✓ Data is encrypted in transit (TLS 1.2+)

✓ Data is encrypted at rest (AES-256)

✓ You can request data deletion

✓ Data is not sold to third parties

✓ Independent security review (SOC 2, ISO 27001)

DATA COLLECTION IS OPTIONAL:

Location access is optional (app works without it)

Camera/photo access is optional (for profile pictures and reviews)

Microphone access is optional (for voice notes)

16.3 Device Permissions Requested

Our app requests the following device permissions:

PHOTO LIBRARY (Optional):

Purpose: Upload profile pictures, service photos, and review photos

Can be denied: Yes, app functions without this permission

PUSH NOTIFICATIONS (Optional):

Purpose: Appointment reminders, booking confirmations

Can be disabled: Yes, via app settings or device settings

MICROPHONE (Optional):

Purpose: Record voice notes in chat conversations

Can be denied: Yes, you can use text chat instead

LOCATION (Optional):

Purpose: Find nearby service providers

Can be denied: Yes, you can search by city/area name instead

When collected: Only when you actively search for services

17. Additional Disclosures

17.1 No Cross-App Tracking

Apple App Tracking Transparency (ATT):

We do not track users across apps and websites owned by other companies for advertising or marketing purposes. We do not request access to your device's advertising identifier (IDFA).

Google Play:

We do not share data with data brokers or use your information for targeted advertising outside our app.

17.2 Referral Program

How It Works:

Users can invite others through a unique referral code

When someone signs up using your code, you may earn rewards

Data Involved:

We generate a unique referral ID (not personally identifiable)

We track which user generated the referral (to award rewards)

We do NOT share your personal information with referred users or vice versa

17.3 No Gift Cards (Feature Removed)

The gift card feature mentioned in earlier versions of our Terms of Use has been removed. We do not currently offer gift cards.

17.4 Reviews and User-Generated Content

When you post a review:

Your name and profile picture are visible to other users

Reviews are public and can be viewed by anyone using the app

SMBs can see reviews posted about their services

You can delete your reviews at any time

If you delete your account, your reviews are also deleted

Review Retention:

Active reviews: Retained indefinitely or until you delete them

Deleted account: Reviews are deleted within 5 business days

18. Compliance Summary

We are committed to compliance with all applicable privacy laws and regulations, including but not limited to:

✓ GDPR (General Data Protection Regulation) - European Union

✓ CCPA/CPRA (California Consumer Privacy Act / California Privacy Rights Act)

✓ COPPA (Children's Online Privacy Protection Act) - United States

✓ Law 172-13 (Dominican Republic Data Protection Law)

✓ Apple App Store Guidelines - Privacy and Data Collection

✓ Google Play Developer Policies - User Data and Privacy

Security Certifications:

✓ SOC 2 Type II

✓ ISO 27001

✓ PCI DSS (via payment processor Azul)

19. Transparency Commitment

We believe in transparency about our data practices. This Privacy Policy is written in clear, plain language to help you understand:

What information we collect and why

How we use and protect your information

Your rights and how to exercise them

How to contact us with questions or concerns

We commit to:

Never selling your personal information

Only collecting data necessary for service delivery

Giving you control over your information

Being transparent about changes to our practices

Responding promptly to your privacy requests

20. Questions and Feedback

We welcome your questions, concerns, and feedback about this Privacy Policy and our privacy practices.

Contact us at:

Email: contact@nyzerapp.com

Phone: +1 849-868-1908

Website: https://www.nyzerapp.com

We typically respond within:

General inquiries: 5 business days

Data subject access requests: 5-30 business days

Security issues: 24 hours

Urgent matters: Same business day

Acknowledgment

By using the Nyzer Service, you acknowledge that you have read and understood this Privacy Policy and agree to its terms.

If you do not agree with this Privacy Policy, please do not use our Service.

END OF PRIVACY POLICY

Document Information:

Version: 2.0

Last Updated: November 12, 2025

Effective Date: November 12, 2025

Next Review: May 12, 2026 (or as needed for legal/operational changes)