PRIVACY POLICY

Effective Date: 2025-12-25
Last Updated: 2025-12-25

---

1. INTRODUCTION

1.1 Who We Are

This Privacy Policy describes how [YOUR COMPANY NAME] ("we", "us", "our"), a company registered under the laws of [YOUR EU COUNTRY] with registered office at [YOUR ADDRESS], collects, uses, stores, and protects your personal data when you use our SubTrack service (the "Service").

Data Controller:
[YOUR COMPANY NAME]
[YOUR ADDRESS]
[YOUR EU COUNTRY]
Email: [YOUR EMAIL]

Data Protection Officer (if applicable):
[DPO NAME OR "Not required - small business exception"]
Email: [DPO EMAIL OR YOUR EMAIL]

1.2 Our Commitment to Privacy

We are committed to protecting your privacy and handling your personal data in accordance with the General Data Protection Regulation (GDPR) (EU) 2016/679 and other applicable data protection laws. This Privacy Policy explains your rights and how we fulfill our obligations under these laws.

1.3 Scope of This Policy

This Privacy Policy applies to:

- Our website located at [YOUR DOMAIN]
- The SubTrack application and services
- All data processing activities related to the Service
- Users worldwide, with particular attention to GDPR compliance for EU/EEA users

1.4 Changes to This Policy

We may update this Privacy Policy from time to time. We will notify you of material changes by:

- Email to your registered address (at least 30 days in advance)
- Prominent notice on our Service
- Updated "Last Updated" date at the top of this document

Your continued use of the Service after changes take effect constitutes acceptance of the updated Privacy Policy.

---

2. WHAT DATA WE COLLECT

2.1 Account Information

When you create an account, we collect:

- **Email address** (used for login, communication, and account recovery)
- **Password** (stored as encrypted hash, never in plain text)
- **Name** (optional - if provided)
- **Subscription tier** (Free, Pro, or Business)
- **Account creation date**
- **Last login information**

Legal Basis: Contract performance (GDPR Art. 6(1)(b))

2.2 Email Account Connection Information

To provide our subscription tracking service, we collect:

- **Email account addresses** you choose to connect
- **IMAP authentication credentials** (app-specific passwords)
    - Stored in encrypted form using AES-256 encryption
    - Never stored in plain text
    - Encrypted before transmission to our servers
- **Email provider information** (Gmail, Outlook, Yahoo, etc.)
- **IMAP server details** (host, port, security settings)
- **Connection status and timestamps**
- **Last scan date and time**

Legal Basis: Contract performance (GDPR Art. 6(1)(b)) - necessary to provide the Service you requested

Important Clarification:
We use IMAP authentication purely for **technical flexibility** to support all email providers (Gmail, Outlook, ProtonMail, Yahoo, custom domains, etc.). This approach allows you to use any email service, not to collect additional data. We only process email data necessary for subscription detection.

2.3 Email Content Data

When scanning your connected email accounts, we process:

- **Email metadata:** sender, subject, date, recipient
- **Email body content:** only text content necessary to identify subscriptions
- **Extracted subscription information:**
    - Merchant/service name
    - Payment amount and currency
    - Billing date and frequency
    - Payment method (last 4 digits only)
    - Plan type (e.g., "Pro", "Business")
    - Invoice links
    - Next payment dates

What We Do NOT Collect:

- Full email content beyond subscription-related messages
- Personal correspondence
- Email attachments (except invoice links)
- Emails unrelated to subscriptions
- Full credit card numbers
- Passwords from emails
- Social security numbers or government IDs

Legal Basis: Contract performance (GDPR Art. 6(1)(b)) - necessary to deliver the core service functionality

Data Minimization Principle:
We strictly adhere to the GDPR data minimization principle. We only process email data necessary to detect and track subscriptions. Once subscription data is extracted, we do not retain full email content.

2.4 Payment Information

If you subscribe to a paid plan, we collect:

- **Billing information:** name, billing address, country
- **Payment method type** (credit card brand, last 4 digits)

- **Transaction IDs** and dates
- **Subscription status** (active, cancelled, past due)

Important: We use third-party payment processors (Stripe) who handle full payment card details. We never see or store complete credit card numbers.

Legal Basis: Contract performance (GDPR Art. 6(1)(b)) and legal obligation (GDPR Art. 6(1)(c)) - tax and accounting requirements

2.5 Usage and Analytics Data

We automatically collect:

- **Device information:** browser type, operating system, device type
- **Usage data:** features used, pages visited, time spent
- **IP address** (for security and fraud prevention)
- **Log data:** access times, error logs, performance metrics
- **Aggregated statistics:** number of scans performed, subscriptions tracked

Legal Basis: Legitimate interests (GDPR Art. 6(1)(f)) - to improve the Service, ensure security, and detect fraud

2.6 Communications Data

We collect data when you contact us:

- **Support inquiries:** email content, attachments you send us
- **Feedback and surveys:** your responses
- **Marketing communications:** email open/click rates (if you opt in)

Legal Basis: Consent (GDPR Art. 6(1)(a)) for marketing; Legitimate interests (GDPR Art. 6(1)(f)) for support and service improvement

2.7 Cookies and Tracking Technologies

We use minimal cookies and tracking:

- **Essential cookies:** Session management, authentication (necessary for Service operation)
- **Functional cookies:** User preferences, language settings
- **Analytics cookies:** Usage statistics (only with consent where required)

We do NOT use:

- Third-party advertising cookies
- Social media tracking pixels

- Cross-site tracking
- Behavioral profiling cookies

For detailed cookie information, see Section 10.

Legal Basis: Consent (GDPR Art. 6(1)(a)) for non-essential cookies; Legitimate interests (GDPR Art. 6(1)(f)) for essential cookies

---

3. HOW WE USE YOUR DATA

3.1 Primary Purposes

We use your personal data to:

Service Delivery:

- Create and manage your account
- Authenticate your identity and secure your account
- Connect to your email accounts via IMAP
- Scan connected email accounts for subscription-related messages
- Extract and organize subscription information
- Display subscription tracking dashboard and analytics
- Send renewal reminders and payment notifications
- Provide customer support

Legal Basis: Contract performance (GDPR Art. 6(1)(b))

3.2 Communication

We use your email address to:

- Send transactional emails (account confirmation, password reset, subscription changes)
- Send service updates and important notices
- Respond to your support inquiries
- Send renewal reminders before billing dates
- Notify you of privacy policy or terms changes

Legal Basis: Contract performance (GDPR Art. 6(1)(b)) for transactional emails; Legitimate interests (GDPR Art. 6(1)(f)) for service updates

Marketing Communications (Optional):

- Send promotional emails about new features or offers

- Share company news and updates
- Conduct surveys and request feedback

Legal Basis: Consent (GDPR Art. 6(1)(a)) - you can opt out at any time

3.3 Service Improvement

We use aggregated and anonymized data to:

- Analyze usage patterns and trends
- Improve subscription detection accuracy
- Develop new features
- Fix bugs and optimize performance
- Conduct internal research and development

Legal Basis: Legitimate interests (GDPR Art. 6(1)(f))

3.4 Security and Fraud Prevention

We process data to:

- Detect and prevent fraud, abuse, and security incidents
- Monitor for suspicious activity
- Enforce our Terms of Service
- Protect our rights and property
- Comply with legal obligations

Legal Basis: Legitimate interests (GDPR Art. 6(1)(f)) and legal obligation (GDPR Art. 6(1)(c))

3.5 Legal Compliance

We may process your data to:

- Comply with legal obligations (tax, accounting, regulatory)
- Respond to lawful requests from authorities
- Protect against legal claims
- Enforce our legal rights

Legal Basis: Legal obligation (GDPR Art. 6(1)(c)) and legitimate interests (GDPR Art. 6(1)(f))

---

4. DATA SHARING AND DISCLOSURE

4.1 Third-Party Service Providers

We share your data with carefully selected third-party processors who help us operate the Service:

Supabase Inc.

- **Purpose:** Database hosting, data storage, and authentication services
- **Data Shared:** All data described in Section 2 (account info, email credentials, extracted subscription data)
- **Location:** Servers located in EU (specific region selectable)
- **Safeguards:** Data Processing Agreement, GDPR-compliant, encrypted storage
- **Privacy Policy:** https://supabase.com/privacy

N8N GmbH

- **Purpose:** Workflow automation and email processing engine
- **Data Shared:** Email credentials (encrypted), email content during processing, extracted subscription data
- **Location:** EU servers (where available) or with appropriate safeguards
- **Safeguards:** Data Processing Agreement, encrypted transmission, temporary processing only
- **Privacy Policy:** https://n8n.io/legal/privacy

Stripe Inc.

- **Purpose:** Payment processing for subscriptions
- **Data Shared:** Billing information, payment details, transaction records
- **Location:** US with EU operations (Privacy Shield alternative mechanisms)
- **Safeguards:** Standard Contractual Clauses, PCI DSS Level 1 certified
- **Privacy Policy:** https://stripe.com/privacy

StackBlitz (Bolt.new)

- **Purpose:** Application hosting and infrastructure
- **Data Shared:** Usage data, application logs, session information
- **Location:** Global CDN with EU presence
- **Safeguards:** Industry-standard security practices
- **Privacy Policy:** https://stackblitz.com/privacy-policy

Email Providers (Gmail, Outlook, Yahoo, etc.)

- **Purpose:** IMAP connection to retrieve emails
- **Data Shared:** IMAP credentials you provide
- **Location:** Varies by provider
- **Safeguards:** Encrypted connections (TLS/SSL), app-specific passwords (not main account passwords)

4.2 Data Processing Agreements

We have entered into Data Processing Agreements (DPAs) with all third-party processors that comply with GDPR Article 28 requirements, ensuring they:

- Process data only on our documented instructions
- Implement appropriate security measures
- Assist with data subject rights requests
- Delete or return data upon termination
- Maintain records of processing activities

4.3 No Data Selling

We **DO NOT** and **WILL NEVER**:

- Sell your personal data to third parties
- Share your data for advertising purposes
- Use your email content for any purpose other than subscription detection
- Share your subscription data with merchants or service providers
- Allow third parties to access your email accounts

4.4 Legal Disclosures

We may disclose your data if required by law:

- In response to valid legal process (court order, subpoena, warrant)
- To comply with applicable laws and regulations
- To protect our rights, property, or safety
- To protect users or the public from harm
- In connection with legal claims or disputes

When legally permitted, we will notify you of such requests and challenge overly broad requests.

4.5 Business Transfers

If we are involved in a merger, acquisition, bankruptcy, or sale of assets, your data may be transferred. We will notify you via email and/or prominent notice on our Service before your data is transferred and becomes subject to a different privacy policy.

---

5. INTERNATIONAL DATA TRANSFERS

5.1 Data Storage Locations

Your data is primarily stored on servers located in the **European Union**.

Specifically:

- **Supabase:** EU region (selectable - we choose EU-based data centers)
- **N8N:** EU servers where available
- **Stripe:** EU operations with data localization where possible

5.2 Transfers Outside the EU/EEA

Some of our service providers may process data outside the EU/EEA. When this occurs, we ensure appropriate safeguards are in place:

Safeguards Used:

- **Standard Contractual Clauses (SCCs):** EU Commission-approved contractual terms
- **Adequacy Decisions:** Transfers only to countries deemed adequate by EU Commission
- **Additional Security Measures:** Encryption, access controls, data minimization
- **Binding Corporate Rules:** For processors with approved BCRs

Specific Transfers:

- **Stripe (US):** Uses SCCs and supplementary measures post-Schrems II
- **StackBlitz (US):** Limited data exposure, primarily infrastructure services

5.3 Your Rights Regarding Transfers

You have the right to:

- Obtain information about transfers to third countries
- Request a copy of the safeguards in place
- Object to transfers in certain circumstances
- Lodge a complaint with your supervisory authority

---

6. DATA SECURITY

6.1 Security Measures

We implement industry-standard technical and organizational measures to protect your data:

Technical Safeguards:

- **Encryption in Transit:** All data transmitted via TLS 1.2+ (HTTPS)

- **Encryption at Rest:** Database encrypted using AES-256
- **Email Credential Encryption:** IMAP passwords encrypted before storage using envelope encryption
- **Password Hashing:** Account passwords hashed using bcrypt with salt
- **Secure Authentication:** Multi-factor authentication available
- **Access Controls:** Role-based access, principle of least privilege
- **Firewall Protection:** Network-level security
- **Regular Security Updates:** Automated patching and updates
- **Intrusion Detection:** Monitoring for suspicious activity
- **Data Backups:** Regular encrypted backups with geographic redundancy

Organizational Safeguards:

- **Staff Training:** Security awareness and GDPR training
- **Confidentiality Agreements:** All personnel bound by confidentiality
- **Access Logging:** Audit trails of data access
- **Incident Response Plan:** Documented breach response procedures
- **Regular Security Audits:** Periodic security reviews
- **Vendor Management:** Due diligence on all processors

6.2 Encryption Details

IMAP Credentials Encryption:

- Client-side encryption before transmission
- Envelope encryption methodology
- Keys stored separately from encrypted data
- Automated key rotation
- No plain-text storage at any point

Why IMAP?
We use IMAP authentication specifically for **technical flexibility** - it allows users to connect any email provider (Gmail, Outlook, ProtonMail, custom domains) without being limited to specific OAuth providers. This is purely a technical decision to serve our users better, not to collect additional data. We encrypt these credentials with the highest security standards.

6.3 Your Security Responsibilities

You play an important role in data security:

- Use strong, unique passwords
- Enable two-factor authentication
- Keep your devices secure
- Use app-specific passwords (not main account passwords) for IMAP
- Report suspicious activity immediately

- Log out from shared devices
- Keep your email account secure

6.4 Data Breach Notification

In the event of a data breach affecting your personal data:

- We will notify relevant supervisory authorities within **72 hours** of discovery (as required by GDPR)
- We will notify affected users **without undue delay** via email
- We will provide information about the breach, its impact, and remedial actions
- We will take immediate steps to contain and remediate the breach

---

7. DATA RETENTION

7.1 Retention Periods

We retain your data only as long as necessary for the purposes described in this Privacy Policy:

Active Accounts:

- Account information: For the duration of your account
- Email credentials: Until you disconnect the email account
- Subscription data: While your account is active
- Usage logs: 12 months
- Support communications: 24 months

Cancelled/Inactive Accounts:

- Free accounts: Data deleted after 12 months of inactivity
- Paid accounts: Data retained for 30 days after cancellation, then deleted
- Billing records: 7 years (legal requirement for tax/accounting)
- Aggregated analytics: Retained indefinitely (anonymized)

Specific Data Types:

- Email credentials: Deleted immediately upon disconnection or account deletion
- Extracted subscription data: 30 days after account deletion
- Payment information: Retained by Stripe per their retention policy and legal requirements
- Support tickets: 24 months after resolution

7.2 Legal Retention Requirements

Some data must be retained longer to comply with legal obligations:

- Tax and accounting records: 7 years
- Records subject to legal hold or investigation: Until resolved
- Data necessary for legal claims: Until statute of limitations expires

7.3 Data Deletion

When retention periods expire or you request deletion:

- Data is securely deleted from production systems within 30 days
- Backup copies are deleted within 90 days
- Data is rendered unrecoverable through secure deletion methods
- Some aggregated, anonymized data may be retained indefinitely for statistical purposes

---

8. YOUR RIGHTS UNDER GDPR

As a data subject under GDPR, you have the following rights:

8.1 Right of Access (Art. 15)

You have the right to:

- Confirm whether we process your personal data
- Obtain a copy of your personal data
- Receive information about how we process your data

How to exercise: Contact us at [YOUR EMAIL] with "Access Request" in the subject line.
Response time: Within 30 days
Cost: Free (first request); reasonable fee for manifestly unfounded or excessive requests

8.2 Right to Rectification (Art. 16)

You have the right to:

- Correct inaccurate personal data
- Complete incomplete personal data

How to exercise: Update your account settings or contact us at [YOUR EMAIL]
Response time: Within 30 days
Cost: Free

8.3 Right to Erasure / "Right to be Forgotten" (Art. 17)

You have the right to request deletion of your data when:

- Data is no longer necessary for the purposes collected
- You withdraw consent and there's no other legal basis
- You object to processing and there are no overriding legitimate grounds
- Data was unlawfully processed
- Legal obligation requires erasure

Exceptions: We may refuse deletion if data is necessary for:

- Legal compliance
- Legal claims or defense
- Exercise of freedom of expression
- Public interest or official authority

How to exercise: Account settings > Delete Account, or contact [YOUR EMAIL]
Response time: Within 30 days
Cost: Free

8.4 Right to Restriction of Processing (Art. 18)

You have the right to restrict processing when:

- You contest the accuracy of data (during verification)
- Processing is unlawful but you don't want deletion
- We no longer need the data but you need it for legal claims
- You've objected to processing (pending verification)

How to exercise: Contact us at [YOUR EMAIL]
Response time: Within 30 days
Cost: Free

8.5 Right to Data Portability (Art. 20)

You have the right to:

- Receive your data in a structured, commonly used, machine-readable format (JSON/CSV)
- Transmit your data to another controller

Applies to: Data you provided, processed based on consent or contract, processed by automated means

How to exercise: Account settings > Export Data, or contact [YOUR EMAIL]
Response time: Within 30 days
Cost: Free

8.6 Right to Object (Art. 21)

You have the right to object to processing based on:

- Legitimate interests (Art. 6(1)(f))
- Direct marketing (absolute right - we must stop immediately)
- Scientific/historical research or statistics

How to exercise: Contact us at [YOUR EMAIL] or use unsubscribe links in emails
Response time: Immediate for marketing; 30 days for other objections
Cost: Free

8.7 Right to Withdraw Consent (Art. 7(3))

Where processing is based on consent, you have the right to:

- Withdraw consent at any time
- Withdraw as easily as it was given

Note: Withdrawal doesn't affect lawfulness of processing before withdrawal.

How to exercise: Account settings or contact [YOUR EMAIL]
Response time: Immediate
Cost: Free

8.8 Right to Lodge a Complaint (Art. 77)

You have the right to lodge a complaint with a supervisory authority, particularly:

- In your country of habitual residence
- In your place of work
- In the place of alleged infringement

Your Lead Supervisory Authority (if EU-based company):
[YOUR COUNTRY] Data Protection Authority
Website: [SUPERVISORY AUTHORITY WEBSITE]
Email: [SUPERVISORY AUTHORITY EMAIL]

Other EU Supervisory Authorities: https://edpb.europa.eu/about-edpb/board/members_en

8.9 How to Exercise Your Rights

Primary Method:
Email: [YOUR EMAIL]
Subject: "[GDPR Request Type] - [Your Name]"

Required Information:

- Your full name
- Email address associated with your account
- Specific right you wish to exercise
- Any relevant details or preferences

Verification:
We may ask for identification to verify your identity before processing requests.

No Fee (Usually):
We don't charge fees for most requests. We may charge a reasonable fee for:

- Manifestly unfounded or excessive requests
- Requests for further copies beyond the first

Response Time:
We will respond within **30 days** (may be extended by 60 days for complex requests with notification).

---

9. CHILDREN'S PRIVACY

9.1 Age Restriction

The Service is not intended for individuals under 18 years of age. We do not knowingly collect personal data from children.

9.2 Parental Consent

If you are under 18, you must have parental or guardian consent before using the Service.

9.3 If We Learn We Have Child Data

If we become aware that we have collected data from a child under 18 without parental consent, we will:

- Delete the data immediately
- Terminate the account
- Notify the parent/guardian if contact information is available

9.4 Parents/Guardians

If you believe we may have collected data from your child, contact us immediately at [YOUR EMAIL].

---

10. COOKIES AND TRACKING TECHNOLOGIES

10.1 What Are Cookies?

Cookies are small text files placed on your device when you visit our website. They help us provide a better user experience.

10.2 Cookies We Use

Strictly Necessary Cookies (No Consent Required):

- **Session cookie:** Keeps you logged in
- **Security cookie:** Prevents CSRF attacks
- **Preference cookie:** Stores language and region settings

Functional Cookies (Consent Required in Some Jurisdictions):

- **Remember me:** Keeps you logged in across sessions
- **UI preferences:** Dashboard layout, theme preferences

Analytics Cookies (Consent Required):

- **Usage statistics:** Pages visited, features used, time spent
- **Performance monitoring:** Load times, error rates

We DO NOT Use:

- Third-party advertising cookies
- Social media tracking pixels (Facebook, Twitter, etc.)
- Cross-site tracking cookies
- Behavioral profiling cookies

10.3 Third-Party Cookies

The Service does not use third-party cookies except:

- **Stripe:** Payment processing (necessary for service)

10.4 Managing Cookies

You can control cookies through:

- **Browser settings:** Most browsers allow you to refuse or delete cookies
- **Our cookie banner:** Accept or reject non-essential cookies
- **Opt-out links:** For specific analytics services

Note: Disabling necessary cookies may prevent you from using the Service.

10.5 Do Not Track (DNT)

We respect Do Not Track signals. If your browser sends a DNT signal, we will not use analytics or tracking cookies.

---

11. AUTOMATED DECISION-MAKING AND PROFILING

11.1 No Automated Decisions

We do **NOT** use automated decision-making or profiling that produces legal effects or similarly significantly affects you.

11.2 Subscription Detection

Our subscription detection algorithms automatically scan emails, but:

- This is purely functional (not profiling)
- Does not make decisions about you
- You maintain full control
- Results are reviewable and editable

---

12. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

12.1 High-Risk Processing

We have conducted a Data Protection Impact Assessment (DPIA) for the following high-risk processing activities:

- Collection and processing of email account credentials
- Access to and processing of email content
- Automated email scanning and analysis

12.2 DPIA Conclusions

Our DPIA concluded that:

- Risks are mitigated through strong encryption
- Data minimization principles are strictly followed
- User rights are fully respected
- Processing is necessary for the service
- No high risks remain after mitigation

12.3 Requesting DPIA Summary

You may request a summary of our DPIA by contacting [YOUR EMAIL].

---

13. SPECIFIC INFORMATION FOR EU/EEA USERS

13.1 Legal Bases for Processing

We process your data under the following legal bases:

Data Type	Legal Basis	GDPR Article
Account information	Contract	Art. 6(1)(b)
Email credentials	Contract	Art. 6(1)(b)
Email content	Contract	Art. 6(1)(b)
Payment data	Contract + Legal obligation	Art. 6(1)(b) + (c)
Usage data	Legitimate interests	Art. 6(1)(f)
Marketing	Consent	Art. 6(1)(a)
Security/fraud	Legitimate interests	Art. 6(1)(f)

13.2 Legitimate Interests

Where we rely on legitimate interests (Art. 6(1)(f)), our interests include:

- Providing secure and reliable service
- Improving user experience
- Preventing fraud and abuse

- Protecting our legal rights
- Business operations and administration

We have balanced these interests against your rights and freedoms.

13.3 Adequacy of Protection

For data processed outside the EU/EEA, we ensure adequate protection through:

- Standard Contractual Clauses approved by EU Commission
- Adequacy decisions by EU Commission
- Supplementary measures (encryption, access controls)

---

14. SPECIFIC INFORMATION FOR NON-EU USERS

14.1 California Residents (CCPA/CPRA)

If you are a California resident, you have additional rights under the California Consumer Privacy Act:

- Right to know what personal information is collected
- Right to know if personal information is sold or disclosed
- Right to say no to sale of personal information (we don't sell data)
- Right to delete personal information
- Right to non-discrimination for exercising your rights

California Privacy Rights Requests: [YOUR EMAIL]

14.2 UK Residents (UK GDPR)

UK residents have the same rights as EU residents under UK GDPR. Our UK supervisory authority is the Information Commissioner's Office (ICO): https://ico.org.uk

14.3 Other Jurisdictions

We comply with applicable data protection laws in all jurisdictions where we operate. If your jurisdiction has specific requirements not addressed here, please contact us.

---

15. CONTACT US

15.1 Privacy Questions

If you have questions about this Privacy Policy or our data practices:

Email: [YOUR EMAIL]
Subject Line: "Privacy Inquiry"
Response Time: Within 5 business days

15.2 Data Protection Officer (if applicable)

DPO Email: [DPO EMAIL]
[If you're a small business, you may write: "As a small business, we are not required to appoint a DPO under GDPR Article 37, but our Privacy team can be reached at [YOUR EMAIL]"]

15.3 Mailing Address

[YOUR COMPANY NAME]
[YOUR ADDRESS]
[YOUR CITY, POSTAL CODE]
[YOUR EU COUNTRY]

15.4 Supervisory Authority

If you're unhappy with how we handle your data, you can lodge a complaint with your supervisory authority:

[YOUR COUNTRY] Supervisory Authority:
[NAME OF AUTHORITY]
[ADDRESS]
Website: [WEBSITE]
Email: [EMAIL]

15.5 Representative in the EU (if applicable)

[If you're NOT based in the EU but serve EU customers, you may need an EU representative under GDPR Art. 27. If you ARE in the EU, this section is not needed.]

---

16. TRANSPARENCY COMMITMENTS

16.1 Our Promises

We commit to:

- Being transparent about data practices
- Collecting only necessary data
- Using data only for stated purposes
- Protecting data with strong security
- Respecting your rights
- Responding promptly to requests
- Notifying you of breaches
- Never selling your data

16.2 Security Updates

We will maintain a security page at [YOUR DOMAIN]/security with:

- Security best practices
- Latest security updates
- How to report vulnerabilities
- Security contact information

16.3 Transparency Reports

We may publish annual transparency reports including:

- Number of data subject requests received and fulfilled
- Data breach incidents (if any)
- Government data requests (if any)
- Service improvements based on privacy feedback

---

17. LEGAL BASIS JUSTIFICATION

17.1 Why We Process Email Content

We process email content based on **contract performance** (GDPR Art. 6(1)(b)) because:

- You explicitly requested this service
- Scanning emails is the core functionality
- We cannot provide the service without email access
- Processing is necessary to fulfill our contractual obligations

17.2 Why We Use IMAP

We use IMAP authentication for **technical flexibility**, not data collection:

- Allows connection to any email provider (Gmail, Outlook, ProtonMail, Yahoo, custom domains)
- Provides universal compatibility
- Enables users to choose their preferred email service
- Does not grant us access to data beyond what's necessary for subscription detection
- We could use OAuth, but it would limit supported email providers significantly

17.3 Proportionality

Our processing is proportionate because:

- We use data minimization (only subscription-related emails)
- We implement strong encryption
- We provide transparency about what we access
- You maintain full control (can disconnect anytime)
- Processing is limited to stated purposes

ACKNOWLEDGMENT

By using the Service, you acknowledge that you have read and understood this Privacy Policy and consent to the collection, use, and disclosure of your personal data as described herein.

Version: 1.0
Effective Date: 2025-12-25
Last Updated: 2025-12-25

This Privacy Policy was last updated on 2025-12-25. We recommend reviewing it periodically for any changes.