



verifalia

Privacy Policy

Last updated October 23, 2025

INTRODUCTION

Your privacy matters to us. This Privacy Policy explains how Verifalia collects, uses, and protects your personal information when you use our email verification services. Please read it carefully to understand your rights and how we safeguard your data.

1. INTRODUCTION

1.1 Who We Are

This Privacy Policy is provided by **Cobisi Research**, operating under the trade name **Verifalia**, a company established under Italian law with its registered office at:

Cobisi Research

Via Della Costituzione, 31
35010 Vigonza (PD)
Italy, European Union
VAT ID: IT04391160282

Website: <https://verifalia.com>

Email: support@verifalia.com

1.2 What This Policy Covers

This Privacy Policy describes how Verifalia collects, uses, stores, shares, and protects your personal information when you:

- Visit our websites (<https://verifalia.com> and <https://app.verifalia.com>);
- Register for and use our email verification services (the "**Services**");
- Communicate with us (via email, support tickets, or chat);
- Subscribe to our newsletters or marketing communications.

Important Distinction:

- **This Privacy Policy** governs personal information about **you** (our Customer) that we collect when you register for and use our Services. In this context, **Verifalia acts as a data controller**.
- **Email addresses you verify** using our Services are governed by our **Data Processing Addendum (DPA)**, available <https://verifalia.com/legal/data-processing-addendum>. For email verification data, **you act as the controller** and **Verifalia acts as a processor** processing data on your behalf.

1.3 Your Consent

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

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

1.4 Scope and Applicability

This Privacy Policy applies to personal information collected by Verifalia as a **data controller**. It does not apply to:

- **Email verification data** (email addresses submitted for verification) - covered by our Data Processing Addendum;
- **Third-party websites or services** linked from our website or Services - such third parties have their own privacy policies.

2. INFORMATION WE COLLECT

We collect personal information in the following categories:

2.1 Information You Provide Directly

Account Registration Information:

When you create a Verifalia account, we collect:

- **Full name** (required)
- **Email address** (required) - also used as your default username
- **Username** (required) - defaults to your email address
- **Password** (required) - stored in hashed format using bcrypt; we never store passwords in plaintext

- **Country** (required) - for tax and invoicing purposes
- **Address** (required) - for tax and invoicing purposes

Business Customer Information (if you register as a business):

- **Company name** (required)
- **VAT ID / Tax ID** (required)

Account Settings and Preferences:

- Default settings for email verifications
- Data retention period preferences
- User permissions and access controls
- Email notification preferences (which newsletters and updates you wish to receive)

Payment and Billing Information:

- **Transaction history** (records of your purchases)
- **Invoices** (generated for your purchases and retained for tax compliance)

Note: Payment card details are processed and stored by our third-party payment processors (Stripe Inc.). Verifalia does not store complete payment card numbers. If you pay via PayPal, you are redirected to PayPal's website and we do not receive or store your PayPal credentials.

2.2 Information Collected Automatically

Usage and Analytics Data:

When you use our Services, we automatically collect:

- **IP address** (for security and fraud prevention purposes)
- **Browser type** (collected during account registration)
- **Login timestamps** (for security purposes)
- **Usage statistics** (API call volumes, verification volumes, features used) - for analytics and service improvement

Communication Data:

- **Support tickets** and customer service communications
- **Email correspondence** with Verifalia

- **Chat logs** (if you use our live chat support feature)

2.3 Information from Third Parties

Profile Photos:

We do not store profile photos or avatars directly. If you wish to display a profile photo, we use [Gravatar](#), which retrieves your photo based on your email address. Please refer to Gravatar's privacy policy for information on how they handle your data.

2.4 Cookies and Tracking Technologies

Our website and Services use cookies and similar tracking technologies. For detailed information about our use of cookies, please see our **Cookie Policy** at <https://verifalia.com/legal/cookie-policy>.

Note: We do not use cookies directly for tracking, but third-party services integrated into our website (such as our chat widget and Google Analytics) may use cookies. These are described in our Cookie Policy.

2.5 Information We Do NOT Collect

We do **not** knowingly collect:

- **Special categories of personal data** (racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, sex life, or sexual orientation);
- **Personal data of children** under the age of 16 (or the applicable age of digital consent in your jurisdiction);
- **Payment card numbers** (processed by Stripe; we receive only tokenized references).

3. HOW WE USE YOUR INFORMATION

We use your personal information for the following purposes:

3.1 To Provide and Manage the Services

- Create and manage your Verifalia account
- Authenticate your identity and grant access to the Services
- Process your email verification requests
- Generate and deliver Verification Results

- Enable you to configure account settings, user permissions, and preferences
- Manage your subscription plan and billing cycle

3.2 To Process Payments and Billing

- Process payments for subscription plans and Credit Pack purchases
- Generate invoices and receipts
- Manage your billing information and payment methods
- Handle refunds and chargebacks (where applicable)
- Comply with tax and accounting obligations

3.3 To Provide Customer Support

- Respond to your inquiries, support requests, and technical issues
- Troubleshoot problems with your account or the Services
- Communicate with you about service-related matters

3.4 To Ensure Security and Prevent Fraud

- Monitor for suspicious activity, unauthorized access, or security threats
- Detect and prevent fraud, abuse, or misuse of the Services
- Enforce our Terms of Service and Acceptable Use Policy
- Maintain audit logs for security and compliance purposes
- Protect the rights, property, and safety of Verifalia, our customers, and others

3.5 To Improve and Optimize the Services

- Analyze usage patterns and trends (in aggregate and anonymized form)
- Improve the performance, reliability, and accuracy of our email verification algorithms
- Develop new features and services
- Conduct research and development (including AI/ML model training and improvement)

3.6 To Comply with Legal Obligations

- Comply with applicable laws, regulations, and legal processes
- Respond to requests from government authorities, courts, or regulatory bodies

- Maintain records required by tax, accounting, and anti-money laundering laws
- Fulfill our obligations under data protection laws

3.7 To Send You Communications

Transactional Communications (cannot be disabled):

- Account confirmation and verification emails
- Password reset and security alerts
- Billing notifications, invoices, and payment confirmations
- Service updates, maintenance notices, and critical security alerts
- Notifications regarding changes to our Terms of Service or Privacy Policy

Marketing Communications (can be disabled):

- Promotional offers and special discounts

You can manage your email notification preferences through your account settings. However, you cannot opt out of transactional communications (critical account and billing notifications) without terminating your account.

3.8 To Enforce Our Terms and Protect Our Rights

- Investigate and address violations of our Terms of Service
- Protect our intellectual property rights
- Defend against legal claims or disputes
- Enforce our agreements and policies

4. LEGAL BASIS FOR PROCESSING (GDPR)

Under the **General Data Protection Regulation (GDPR)**, we are required to inform you of the legal basis for processing your personal data. We process your personal information under the following legal bases:

Purpose	Legal Basis	GDPR Article
---------	-------------	--------------

Account creation and management	Performance of contract	Article 6(1)(b)
Providing the Services	Performance of contract	Article 6(1)(b)
Billing and payment processing	Performance of contract	Article 6(1)(b)
Customer support	Performance of contract	Article 6(1)(b)
Security and fraud prevention	Legitimate interests	Article 6(1)(f)
Service improvement and analytics	Legitimate interests	Article 6(1)(f)
Enforcing Terms of Service	Legitimate interests	Article 6(1)(f)
Compliance with tax, accounting, and legal obligations	Legal obligation	Article 6(1)(c)
Marketing communications (newsletters, promotional emails)	Consent	Article 6(1)(a)

Legitimate Interests:

Where we rely on legitimate interests as our legal basis, our legitimate interests include:

- Ensuring the security and integrity of our Services
- Preventing fraud, abuse, and unauthorized access
- Improving our Services and developing new features
- Understanding how customers use our Services to optimize performance
- Enforcing our legal rights and obligations

We have assessed that these interests are not overridden by your interests, rights, or freedoms, given the nature of the data processed and the safeguards we have implemented.

Consent:

Where we rely on your consent (such as for marketing communications), you have the right to withdraw your consent at any time by adjusting your preferences in your account settings at <https://app.verifalia.com>.

5. HOW WE SHARE YOUR INFORMATION

We do **not** sell, rent, or lease your personal information to third parties for marketing purposes.

We may share your personal information with the following categories of recipients:

5.1 Service Providers and Processors

We engage trusted third-party service providers to support our business operations. These providers process personal data on our behalf and are contractually obligated to protect your information and use it only for the purposes we specify.

Payment Processors:

- Stripe Inc. - Processes credit and debit card payments in accordance with PCI DSS standards. Stripe's privacy policy is available at <https://stripe.com/privacy>.

Note: If you pay via PayPal, you are redirected to PayPal's website. We do not receive or store your PayPal credentials. PayPal processes your payment information in accordance with its own privacy policy.

Cloud Infrastructure and Hosting Providers:

- **Hetzner Online GmbH** (Germany)
- **Amazon Web Services, Inc. (AWS)** (Germany - Region: eu-central-1)
- **myLoc managed IT AG** (Germany)
- **M247 Europe S.R.L.** (Germany)

These providers host our servers and infrastructure but do not have access to or visibility into your personal data in unencrypted form. All data is stored exclusively within the **European Economic Area (Germany)**.

Email Service Provider:

- **Amazon Simple Email Service (SES)** - Sends transactional emails, invoices, password resets, and notifications on our behalf. Amazon SES processes only your email address for the purpose of email delivery.

5.2 Professional Advisors

We may share your personal information with:

- **Accountants and tax advisors** - For financial reporting, tax compliance, and audit purposes
- **Legal counsel** - For legal advice and representation (only when necessary)

These advisors are bound by professional confidentiality obligations.

5.3 Government Authorities and Legal Compliance

We may disclose your personal information to government authorities, regulatory bodies, or law enforcement agencies when required by law or when necessary to:

- Comply with legal obligations, court orders, or regulatory requests
- **Italian Tax Authority (Agenzia delle Entrate)** - For VAT/tax compliance and invoicing (we share business name, address, VAT ID, and invoice details as required by Italian tax law)
- Enforce our Terms of Service or protect our legal rights
- Protect the safety, rights, or property of Verifalia, our customers, or the public
- Investigate fraud, security incidents, or violations of our policies

5.4 Business Transfers

In the event of a merger, acquisition, reorganization, sale of assets, or bankruptcy, your personal information may be transferred to the successor entity or acquirer. We will notify you of any such transfer and any choices you may have regarding your personal information.

5.5 With Your Consent

We may share your personal information with third parties where you have provided your explicit consent to such sharing.

5.6 No Sale of Personal Data

We do not sell your personal data. We do not share your personal data with third parties for their own marketing purposes or for monetary or other valuable consideration.

6. DATA RETENTION

We retain your personal information for as long as necessary to fulfill the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law.

6.1 Account Data

While Your Account is Active:

We retain your account information (name, email, username, address, company details, account settings) for as long as your account remains active.

After Account Termination:

When you terminate your account (by using the "Close Account" feature in the app or by contacting us), we **anonymize** your personal data. Anonymized data does not identify you and is not considered personal data under GDPR.

6.2 Billing and Tax Records

Invoices and billing records are retained for **10 years** from the date of issuance, as required by Italian tax and accounting law (Decreto del Presidente della Repubblica 26 ottobre 1972, n. 633).

6.3 Usage Logs and Analytics

Usage logs (IP addresses, login timestamps, API usage statistics) are retained for **2 years** from the date of collection for security, fraud prevention, and analytics purposes.

6.4 Support Communications

Support tickets, email correspondence, and chat logs are retained for **2 years** from the date of the communication for customer support, quality assurance, and legal compliance purposes.

6.5 Marketing Consent Records

Marketing consent records (evidence of your consent to receive newsletters) are retained while your account is active. Upon account termination, these records are anonymized.

6.6 Legal Retention

We may retain personal information for longer periods where required by law, regulation, legal process, or to establish, exercise, or defend legal claims.

7. YOUR PRIVACY RIGHTS

Depending on your location and applicable privacy laws, you may have the following rights regarding your personal information:

7.1 Rights Under GDPR (EU/EEA Residents)

If you are located in the European Union or European Economic Area, you have the following rights under the GDPR:

Right of Access (Article 15):

You have the right to obtain confirmation as to whether we process your personal data and, if so, to access your personal data and receive information about how we process it.

Right to Rectification (Article 16):

You have the right to request correction of inaccurate or incomplete personal data.

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

You have the right to request deletion of your personal data in certain circumstances (such as when the data is no longer necessary for the purposes for which it was collected, or when you withdraw consent).

Right to Restriction of Processing (Article 18):

You have the right to request restriction of processing of your personal data in certain circumstances (such as when you contest the accuracy of the data or object to processing).

Right to Data Portability (Article 20):

You have the right to receive your personal data in a structured, commonly used, and machine-readable format (where technically feasible) and to transmit that data to another controller.

Note: Currently, account data export functionality is not available through the Services. If you wish to exercise your right to data portability, please use the "Request support" feature in the app, and we will provide your data in a suitable format.

Right to Object (Article 21):

You have the right to object to processing of your personal data based on legitimate interests or for direct marketing purposes.

Right to Withdraw Consent (Article 7(3)):

Where we process your personal data based on consent (such as for marketing communications), you have the right to withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

Right Not to Be Subject to Automated Decision-Making (Article 22):

You have the right not to be subject to decisions based solely on automated processing (including profiling) that produce legal effects concerning you or similarly significantly affect you. See Section 10 for information about our use of automated decision-making.

7.2 How to Exercise Your Rights

You can exercise most of your rights directly through the Services:

- **Access and Rectify:** Log in to your account at <https://app.verifalia.com> and view or update your account information, settings, and preferences.
- **Erase:** Use the "Close Account" feature in your account settings to terminate your account and anonymize your personal data.
- **Restrict:** Disable access for specific users through the user management interface.
- **Object / Withdraw Consent:** Adjust your email notification preferences in your account settings to opt out of marketing communications.

For other requests or assistance, please contact us:

- **Preferred method:** Use the "Request support" feature in the app at <https://app.verifalia.com>
- **Alternative:** Email support@verifalia.com

We will respond to your request without undue delay and in any event within **one (1) month** of receipt, as required by GDPR Article 12(3). In complex cases, we may extend this period by an additional two months and will inform you of any such extension.

7.3 Rights Under Other Privacy Laws

If you are located outside the EU/EEA, you may have similar rights under applicable privacy laws in your jurisdiction (such as CCPA in California, LGPD in Brazil, or PIPEDA in Canada). Please contact us using the methods above to exercise such rights.

7.4 Verification of Identity

To protect your privacy and security, we may require you to verify your identity before processing requests to access, rectify, or delete your personal data.

7.5 No Fee

You will not have to pay a fee to exercise your privacy rights. However, we may charge a reasonable fee or refuse to comply with your request if it is clearly unfounded, excessive, or repetitive.

8. SECURITY MEASURES

We take the security of your personal information seriously and have implemented appropriate technical and organizational measures to protect your data against unauthorized access, accidental loss, alteration, or destruction.

8.1 Technical Security Measures

Encryption:

- **In Transit:** All data transmitted between your device and our Services is encrypted using **Transport Layer Security (TLS)**.
- **At Rest:** Personal data stored in our databases is encrypted using **AES-256** encryption or equivalent industry-standard encryption.

Authentication and Access Controls:

- **Password Security:** Passwords are hashed using **bcrypt** with unique salts and are never stored in plaintext.
- **Multi-Factor Authentication (MFA):** Available for your account to add an extra layer of security.
- **Role-Based Access Control:** Our personnel have access to personal data only on a strict need-to-know basis.
- **Client Certificate Authentication:** Advanced authentication options available for API access (X.509 TLS).

Infrastructure Security:

- **Firewalls and Intrusion Detection:** Our systems are protected by firewalls and intrusion detection/prevention systems.
- **Security Monitoring:** We continuously monitor for suspicious activity, unauthorized access attempts, and security threats.
- **Regular Updates:** We apply security patches and updates promptly to address vulnerabilities.

8.2 Organizational Security Measures

Personnel:

- All Verifalia personnel with access to personal data are bound by strict confidentiality obligations.

- Personnel receive regular training on data protection and security best practices.

Data Centers:

Our infrastructure is hosted in certified, secure data centers located in **Germany (European Union)** operated by Hetzner, AWS, myLoc, and M247. These facilities feature:

- 24/7 video surveillance and on-site security personnel
- Biometric access controls and electronic access terminals
- Redundant power supplies, climate control, and fire suppression systems
- Physical security measures compliant with industry standards

Audits and Assessments:

We conduct regular:

- Vulnerability assessments and penetration testing
- Security audits and compliance reviews
- Monitoring and incident response exercises

8.3 No Guarantee

While we implement industry-standard security measures, no method of electronic storage or transmission over the internet is 100% secure. We cannot guarantee absolute security of your personal information.

Your Responsibility:

You are responsible for:

- Maintaining the confidentiality of your account credentials (username and password)
- Enabling multi-factor authentication and other available security features
- Notifying us immediately of any unauthorized access to your account

9. INTERNATIONAL DATA TRANSFERS

9.1 Data Storage Location

All personal information we collect is **processed and stored exclusively within the European Economic Area (EEA)**, specifically in **Germany**.

We do not transfer your personal data outside the EEA for processing or storage.

9.2 Access from Outside the EEA

If you access our Services from outside the EEA (such as from the United States, Asia, or other regions), your personal information will be transferred to and processed in the EEA (Germany) when you submit it to us.

By using our Services from outside the EEA, you acknowledge and consent to such transfer and processing in accordance with this Privacy Policy and applicable data protection laws.

9.3 Safeguards

Where personal data is transferred internationally (such as when you access your account from outside the EEA), we rely on the following safeguards:

- **Your explicit consent** to the transfer (by accepting this Privacy Policy and using the Services);
- **Performance of contract** (the transfer is necessary to provide the Services you have requested);
- **Standard Contractual Clauses** (where applicable under the circumstances of the transfer).

10. AUTOMATED DECISION-MAKING

10.1 Fraud Detection and Security

We use **automated decision-making systems** (including algorithms and AI-based tools) to detect and prevent fraud, abuse, and security threats.

These systems may automatically:

- Flag suspicious account registrations or login attempts
- Block or suspend accounts exhibiting patterns consistent with fraud or abuse
- Throttle or rate-limit API requests that exceed reasonable usage thresholds
- Identify and prevent unauthorized access or misuse of the Services

Legal Basis: Legitimate interests (security and fraud prevention) under GDPR Article 6(1)(f).

10.2 Your Rights

Under GDPR Article 22, you have the right not to be subject to decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you.

If you believe an automated decision has been made regarding your account that significantly affects you, you have the right to:

- Obtain human intervention and review of the decision
- Express your point of view
- Contest the decision

To exercise this right, please contact us using the "Request support" feature in the app or email support@verifalia.com.

11. CHILDREN'S PRIVACY

Our Services are **not intended for use by individuals under the age of 18** (or the applicable age of majority in your jurisdiction).

We do not knowingly collect personal information from children under 16 years of age (or the applicable age of digital consent under GDPR Article 8).

If you are under 18, you may use the Services only with the express written consent of a parent or legal guardian, and such parent or guardian must review and agree to our Terms of Service and this Privacy Policy.

If we become aware that we have collected personal information from a child under the applicable age without proper parental consent, we will take steps to delete such information promptly.

If you believe we have collected information from a child without proper consent, please contact us immediately at support@verifalia.com.

12. CHANGES TO THIS PRIVACY POLICY

12.1 Right to Modify

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or for other operational, legal, or regulatory reasons.

12.2 Notice of Changes

When we make material changes to this Privacy Policy, we will notify you by:

- Updating the "**Last Updated**" date at the top of this document;
- Sending **email notification** to the email address associated with your account;
- Displaying an **in-app notification** when you next log in to the Services; and/or
- Posting a prominent notice on our website.

Material changes will take effect **30 days** after we provide notice, unless a shorter period is required by law.

12.3 Your Continued Use

Your continued use of the Services after the effective date of any changes to this Privacy Policy constitutes your acceptance of the revised Privacy Policy.

If you do not agree to the changes, you must discontinue use of the Services and may terminate your account.

12.4 Review Responsibility

We encourage you to review this Privacy Policy periodically to stay informed about how we protect your information.

13. CONTACT US & DATA PROTECTION OFFICER

13.1 General Inquiries

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

Preferred method:

Use the "**Request support**" feature in the Verifalia app at <https://app.verifalia.com>

Alternative contact:

Email: support@verifalia.com

Postal address:

Cobisi Research
Via Della Costituzione, 31
35010 Vigonza (PD)
Italy, European Union

13.2 Data Protection Officer

Verifalia has appointed a **Data Protection Officer (DPO)** in accordance with GDPR Article 37.

Our DPO is responsible for overseeing our data protection practices and ensuring compliance with applicable privacy laws.

Data Protection Officer:

Efran Cobisi, Chief Technology Officer
Email: dpo@verifalia.com

You may contact our DPO directly regarding:

- Questions about how we process your personal data
- Requests to exercise your privacy rights
- Concerns about our privacy practices or compliance
- Data protection impact assessments
- Complaints or data protection issues

14. APPLICABLE PRIVACY LAWS

Verifalia is committed to compliance with data protection and privacy laws worldwide. We operate in accordance with a comprehensive framework of international privacy regulations, including:

14.1 European Union & EEA

- **Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)**
- **Directive 2002/58/EC - e-Privacy Directive**

14.2 Other Jurisdictions

Our Services are available globally, and we comply with applicable privacy laws in the following jurisdictions:

Americas:

- Argentina: Personal Data Protection Law (Ley 25.326)
- Brazil: Lei Geral de Proteção de Dados (LGPD)
- Canada: Personal Information Protection and Electronic Documents Act (PIPEDA); Anti-Spam Legislation (CASL)
- United States: California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA); Colorado Privacy Act (CPA); Connecticut Data Privacy Act (CTDPA); Montana Consumer Data Privacy Act (MCDPA); Utah Consumer Privacy Act (UCPA); Virginia Consumer Data Protection Act (VCDPA)

Asia-Pacific:

- Australia: Privacy Act 1988 and Australian Privacy Principles (APPs)
- China: Personal Information Protection Law (PIPL)
- Japan: Act on the Protection of Personal Information (APPI)
- Singapore: Personal Data Protection Act (PDPA)
- South Korea: Personal Information Protection Act (PIPA)
- Thailand: Personal Data Protection Act (PDPA)

Middle East & Africa:

- Israel: Privacy Protection Law
- Saudi Arabia: Personal Data Protection Law (PDPL)
- South Africa: Protection of Personal Information Act (POPIA)
- United Arab Emirates: Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data

United Kingdom:

- UK GDPR and Data Protection Act 2018

And any other applicable national, federal, state, provincial, or local data protection and privacy laws.

14.3 Primary Compliance Framework

As a company established in **Italy** (European Union), our primary compliance framework is the **GDPR**, which provides one of the world's strongest and most comprehensive standards for data protection.

Where other jurisdictions impose additional or different requirements, we comply with such requirements to the extent they apply to our processing of your personal data.

15. COMPLAINTS TO SUPERVISORY AUTHORITIES

15.1 Your Right to Complain

Under GDPR and other applicable privacy laws, you have the right to lodge a complaint with a data protection supervisory authority regarding our processing of your personal data.

15.2 Supervisory Authorities

If you are located in Italy or the EU/EEA:

You may lodge a complaint with:

Italian Data Protection Authority (Garante per la protezione dei dati personali)

Piazza Venezia, 11

00187 Roma, Italy

Website: <https://www.garanteprivacy.it>

Email: garante@gpdp.it

Alternatively, if you are located in another EU/EEA Member State, you may lodge a complaint with the supervisory authority in your country of residence or place of work.

If you are located in the United Kingdom:

UK Information Commissioner's Office (ICO)

Wycliffe House, Water Lane

Wilmslow, Cheshire SK9 5AF

United Kingdom

Website: <https://ico.org.uk>

Phone: +44 303 123 1113

If you are located in other jurisdictions:

You may have the right to lodge a complaint with the relevant privacy or data protection authority in your country. Please consult your local authority's website for information on how to file a complaint.

15.3 Contact Us First

While you have the right to lodge a complaint with a supervisory authority at any time, we encourage you to **contact us first** so we can attempt to resolve your concerns directly.

16. ADDITIONAL INFORMATION

16.1 Links to Other Websites

Our website and Services may contain links to third-party websites, services, or resources. This Privacy Policy does not apply to such third-party sites.

We are not responsible for the privacy practices or content of third-party websites. We encourage you to read the privacy policies of any third-party sites you visit.

16.2 California "Do Not Sell"

We do not sell personal information.

If you are a California resident, you have the right under the California Consumer Privacy Act (CCPA) to opt out of the "sale" of your personal information. Because we do not sell personal information, there is no need to opt out.

We do not share your personal information with third parties for cross-context behavioral advertising or other purposes that would constitute a "sale" under CCPA.

16.3 Relationship to Other Policies

This Privacy Policy should be read in conjunction with:

- Our **Terms of Service** at <https://verifalia.com/legal/terms-of-service>
- Our **Data Processing Addendum** at <https://verifalia.com/legal/data-processing-addendum> (applicable when you use our Services to verify email addresses)
- Our **Cookie Policy** at <https://verifalia.com/legal/cookie-policy>

In the event of any conflict between this Privacy Policy and the Data Processing Addendum with respect to email verification data (email addresses you submit for verification), the Data Processing Addendum prevails.

16.4 Language

This Privacy Policy is drafted in English. Any translation is provided for convenience only. In the event of any conflict or inconsistency between the English version and any translation, the **English version shall prevail**.

16.5 Governing Law

This Privacy Policy and any disputes arising out of or related to this Privacy Policy shall be governed by the laws of **Italy**, without regard to its conflict of law principles.

However, your statutory rights under applicable data protection laws (including GDPR) cannot be limited or waived by this choice of law provision.

17. EFFECTIVE DATE

This Privacy Policy is effective as of the "Last Updated" date stated at the top of this document.



Cobisi Research

Via Della Costituzione, 31
35010 – Vigonza
Italy (European Union)

VAT ID: IT04391160282

Website: <https://verifalia.com>

Email: support@verifalia.com