Data Processing Addendum

Last updated October 23, 2025

INTRODUCTION

This Data Processing Addendum ("**DPA**") forms part of and is incorporated into the Terms of Service (the "**Agreement**" or "**Terms**") between Cobisi Research, operating under the trade name Verifalia ("**Verifalia**", "**Processor**", "**we**", "**us**", or "**our**"), and the customer identified in the Agreement ("**Customer**", "**Controller**", or "**you**").

This DPA governs the processing of Personal Data by Verifalia on behalf of Customer in connection with the provision of Verifalia's email verification services (the "**Services**").

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

For the purposes of this DPA, the following definitions apply:

(a) "**Applicable Data Protection Laws**" means all laws and regulations applicable to the processing of Personal Data under this DPA, including **without limitation**:

- **Argentina**: Personal Data Protection Law (Ley 25.326)
- **Australia**: Privacy Act 1988 and Australian Privacy Principles (APPs)
- **Brazil**: Lei Geral de Proteção de Dados (LGPD);
- **Canada**:
  - Canada's Anti-Spam Legislation (CASL);
  - Personal Information Protection and Electronic Documents Act (PIPEDA);
- **China**: Personal Information Protection Law (PIPL)
- **European Union / EEA**:
  - Directive 2002/58/EC (e-Privacy Directive);
  - Regulation (EU) 2016/679 (General Data Protection Regulation) ("GDPR");
- **Israel**: Privacy Protection Law
- **Japan**: Act on the Protection of Personal Information (APPI)
- **Singapore**: Personal Data Protection Act (PDPA)
- **Saudi Arabia**: Personal Data Protection Law (PDPL)
- **South Africa**: Protection of Personal Information Act (POPIA)

- **South Korea**: Personal Information Protection Act (PIPA)
- **Thailand**: Personal Data Protection Act (PDPA)
- **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;
- **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);
- **Any other applicable** national, federal, state, provincial, or local data protection, privacy, or security laws, regulations, or codes of practice.

(b) "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" (and "**Process**"), "**Supervisory Authority**", and "**Special Categories of Personal Data**" shall have the meanings given to them in the GDPR or, where applicable, equivalent terms in other Applicable Data Protection Laws.

(c) "**Customer Data**" means Personal Data submitted by or on behalf of Customer to the Services for Processing by Verifalia, consisting of:

- **Email Addresses**: The email addresses submitted for verification, stored in volatile (RAM-only) memory and automatically deleted upon expiry of the retention period configured by Customer (between 5 minutes and 30 days);
- **Verification Metadata**: Data generated by Verifalia during the verification process, including verification status and deliverability indicators, stored in volatile memory with the same retention period as the associated email addresses and automatically deleted upon expiry;
- **Custom Reference Strings**: Optional non-personal reference identifiers submitted by Customer for internal administrative purposes, stored in volatile (RAM-only) memory with the same retention period as email addresses and automatically deleted upon expiry;
- **IP Addresses**: The IP address of the submitter collected during job submission for security, fraud prevention, and usage analytics purposes, and automatically

anonymized (replaced with the placeholder "0.0.0.0") upon deletion of the associated email addresses;

- **Incidental Personal Data in Optional Fields**: To the extent Customer submits Personal Data in optional metadata fields (job name), such data is stored in Verifalia's database (not volatile RAM) and is automatically deleted when the associated email addresses are deleted.

Customer acknowledges that optional metadata fields (job names) are intended solely for Customer's internal administrative reference and should not contain Personal Data. However, to ensure compliance with Applicable Data Protection Laws, any Personal Data inadvertently or improperly submitted in such fields will be automatically deleted in accordance with this definition when the associated email addresses are deleted.

(d) "**Standard Contractual Clauses**" or "**SCCs**" means:

- For transfers subject to the GDPR: the standard contractual clauses for the transfer of personal data to processors established in third countries adopted by European Commission Decision 2021/914 of 4 June 2021;
- For transfers subject to the UK GDPR: the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office (version B1.0, in force 21 March 2022), or such other transfer mechanism as approved under UK data protection laws.

(e) "**Restricted Transfer**" means a transfer of Personal Data that requires a safeguard under Applicable Data Protection Laws, including transfers from the European Economic Area, United Kingdom, or Switzerland to countries not recognised as providing adequate protection.

(f) "**Services**" has the meaning given to it in the Agreement.

(g) "**Subprocessor**" means any third party appointed by Verifalia to Process Customer Data on behalf of Customer.

(h) All other capitalised terms not defined in this DPA shall have the meanings set forth in the Agreement.

1.2 Interpretation

(a) References to "**Articles**" or "**Annexes**" are to articles of or annexes to this DPA unless otherwise specified.

(b) Headings are for convenience only and do not affect interpretation.

(c) The singular includes the plural and vice versa.

(d) References to "**including**" mean "including without limitation."

(e) This DPA shall be interpreted in a manner consistent with Applicable Data Protection Laws. In the event of any conflict or inconsistency between the provisions of this DPA and Applicable Data Protection Laws, Applicable Data Protection Laws shall prevail.

2. SCOPE AND APPLICABILITY

2.1 Incorporation into Agreement

This DPA is incorporated into and forms part of the Agreement. In the event of any conflict or inconsistency between the provisions of the Agreement and this DPA with respect to the Processing of Personal Data, this DPA shall prevail.

2.2 Scope of DPA

(a) This DPA applies only to the Processing of Customer Data by Verifalia in the course of providing the Services as described in Annex 1.

(b) This DPA does not apply to:

- Personal Data processed by Verifalia as an independent Controller (such as Customer's account registration details, billing information, or usage analytics), which is governed by Verifalia's Privacy Policy available at https://verifalia.com/legal/privacy-policy;
- Payment and billing information processed by third-party payment processors. Payment card information is processed by Stripe Inc. in accordance with PCI DSS standards. If Customer pays via PayPal, payment information is processed by PayPal in accordance with PayPal's terms and privacy policy. Verifalia does not store complete payment card numbers.

(c) **Customer Acting as Processor**: Where Customer processes Personal Data as a Processor on behalf of Customer's own clients (third-party Controllers), Customer represents, warrants, and undertakes that:

i. Customer has obtained all necessary authorizations from the relevant Controller(s) to engage Verifalia as a sub-processor in accordance with GDPR Article 28(2) and (4) or equivalent provisions of other Applicable Data Protection Laws;

ii. Customer has imposed on Verifalia, through this DPA, data protection obligations that are equivalent to or more protective than those imposed on Customer by the relevant Controller(s) in Customer's processor agreement(s) with such Controller(s);

iii. Customer will remain fully liable to the relevant Controller(s) for Verifalia's performance of its obligations under this DPA, in accordance with GDPR Article 28(4);

iv. Customer will make this DPA available to the relevant Controller(s) upon request to demonstrate compliance with Customer's sub-processor obligations.

2.3 Nature of Data Processing

Customer acknowledges and agrees that:

(a) Verifalia Processes Customer Data solely as a Processor on behalf of Customer, who acts as the Controller;

(b) Verifalia does not use Customer Data for any purpose other than providing the Services in accordance with Customer's documented instructions;

(c) The details of the Processing, including the subject matter, duration, nature and purpose of Processing, types of Personal Data, and categories of Data Subjects, are set forth in Annex 1.

2.4 Order of Precedence

In the event of any conflict or inconsistency between the documents comprising this DPA, the following order of precedence applies (highest to lowest):

1. The Standard Contractual Clauses (Annex 4);
2. The main body of this DPA (Articles 1–16);
3. The Annexes to this DPA (other than Annex 4);
4. The Agreement.

3. ROLES AND RESPONSIBILITIES

3.1 Customer as Controller

Customer represents, warrants, and undertakes that:

(a) Customer is a Controller of the Customer Data and is responsible for compliance with all Controller obligations under Applicable Data Protection Laws;

(b) Customer has established and will maintain a lawful basis for the Processing of Customer Data under Applicable Data Protection Laws (such as consent, contractual necessity, legitimate interests, or legal obligation);

(c) Customer has provided, or will provide, all necessary privacy notices to Data Subjects and has obtained all necessary consents, authorisations, and rights to submit Customer Data to Verifalia for Processing as contemplated by this DPA and the Agreement;

(d) Customer's instructions for the Processing of Customer Data, including the submission of Customer Data to the Services, comply with Applicable Data Protection Laws;

(e) Customer is solely responsible for the accuracy, quality, legality, and integrity of Customer Data and the means by which Customer acquired Customer Data;

(f) **Data Localization Compliance**: Customer's submission of Personal Data to the Services (which are hosted exclusively in the European Economic Area, Germany) complies with any applicable data localization, cross-border transfer, or data residency laws in Customer's jurisdiction or the jurisdiction of the Data Subjects. If applicable law requires Personal Data to be stored or processed within a specific jurisdiction (e.g., China, Russia, Indonesia, Vietnam), Customer is solely responsible for ensuring compliance with such requirements and shall not submit such Personal Data to the Services unless Customer has obtained required authorisations, implemented required safeguards, or determined that such laws do not apply to Customer's use of the Services;

(g) **South Korea PIPA Compliance**: If Customer is subject to South Korea's Personal Information Protection Act (PIPA) or Processes Personal Data of individuals located in South Korea, Customer represents and warrants that Customer has:

   i. Obtained any required consents from Data Subjects for the cross-border transfer of Personal Data to Verifalia (located in the EU);

   ii. Provided any required notifications to the Personal Information Protection Commission (PIPC) or fulfilled other PIPA requirements applicable to Controllers; and

   iii. Complied with all applicable PIPA obligations, including consent, notice, and security requirements;

(h) **China PIPL Compliance**: If Customer is subject to China's Personal Information Protection Law (PIPL) or Processes Personal Data of individuals located in China, Customer acknowledges that Customer's submission of such data to Verifalia (located in the EU) constitutes a cross-border transfer of Personal Data subject to PIPL. Customer is solely responsible for:

   i. Obtaining any required security assessment from the Cyberspace Administration of China (CAC);

   ii. Implementing required transfer mechanisms (Standard Contracts, Certification, or other approved mechanisms);

   iii. Providing any required notices to Data Subjects or authorities; and

   iv. Complying with all other applicable PIPL obligations.

Verifalia does not provide legal advice regarding PIPL compliance and does not represent that the Services are compliant with PIPL for Customer's specific use case. Customer should consult with legal counsel if unsure.

3.2 Verifalia as Processor

Verifalia represents, warrants, and undertakes that:

(a) Verifalia acts solely as a Processor of Customer Data on behalf of Customer and will Process Customer Data only on documented instructions from Customer (including as set forth in this DPA and the Agreement), except where required to do so by Applicable Data Protection Laws, in which case Verifalia shall inform Customer of such legal requirement prior to Processing, unless prohibited by law;

(b) Verifalia will comply with all obligations applicable to Processors under Applicable Data Protection Laws;

(c) Verifalia has implemented and will maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in Article 7 and Annex 2;

(d) Verifalia will not Process Customer Data for any purpose other than providing the Services in accordance with this DPA.

3.3 No Sale of Personal Data

Verifalia does not and will not sell, rent, lease, or otherwise disclose Customer Data to third parties for monetary or other valuable consideration. Verifalia does not use Customer Data for Verifalia's own marketing purposes or to build profiles of Data Subjects.

3.3 Customer as Processor (Where Applicable)

Where Customer processes Personal Data as a Processor on behalf of Customer's clients, Customer shall:

(a) Ensure that the representations and warranties set forth in Article 3.1 are fulfilled by the relevant Controller(s) (Customer's clients);

(b) Comply with all applicable Processor obligations under Applicable Data Protection Laws, including GDPR Article 28;

(c) Not instruct Verifalia to Process Customer Data in any manner that would violate the Controller's instructions or Applicable Data Protection Laws.

4. CUSTOMER INSTRUCTIONS AND PROHIBITED DATA

4.1 Processing Instructions

(a) Verifalia shall Process Customer Data only on documented instructions from Customer, unless required to do so by Applicable Data Protection Laws.

(b) Customer's instructions for Processing are documented in this DPA and the Agreement, and include:

- Submission of email addresses and associated data through the Services (via web interface, API, or other documented methods);
- Configuration of verification parameters, data retention periods, and quality settings;
- Access, retrieval, export, and deletion of Verification Results via the Services;
- Any other instructions provided by Customer through the functionality of the Services or in writing to Verifalia's designated contact.

(c) Customer may issue additional written instructions regarding the Processing of Customer Data, provided such instructions are consistent with the terms of this DPA and the Agreement. Verifalia shall comply with such additional instructions unless they require changes to the Services or incur additional costs, in which case the Parties shall agree in writing on the scope, timeline, and any applicable fees before implementation.

(d) If Verifalia reasonably believes that an instruction from Customer violates Applicable Data Protection Laws, Verifalia shall promptly inform Customer and may suspend Processing until the instruction is confirmed, withdrawn, or modified.

4.2 Prohibited Data

(a) Customer shall not submit to the Services, and represents and warrants that Customer Data does not and will not include:

i. **Special Categories of Personal Data** as defined in GDPR Article 9, including Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation;

ii. **Personal Data relating to criminal convictions and offences** as referenced in GDPR Article 10, or equivalent categories of sensitive data under other Applicable Data Protection Laws;

iii. **Personal Data of children** under the age of 16 years (or the lower age of digital consent in the relevant jurisdiction), except where Customer has obtained verifiable parental consent or otherwise has a lawful basis under Applicable Data Protection Laws;

iv. Any **Personal Data that Customer does not have the legal right to Process** or submit to Verifalia under Applicable Data Protection Laws;

v. **Prohibited High-Risk Data**: Customer shall not use the Services or Verification Results:

- For any automated decision-making that produces legal effects concerning, or similarly significantly affects, a natural person (GDPR Article 22), including decisions relating to credit, employment, education, housing, insurance, health care, social benefits, or legal matters;
- In any manner that could subject Verifalia to regulation as a consumer reporting agency under the US Fair Credit Reporting Act (FCRA) or equivalent laws in other jurisdictions;
- To profile, discriminate against, or make inferences about individuals' protected characteristics, behavior, or preferences;
- In violation of any applicable anti-discrimination, consumer protection, or fair lending laws.

vi. **Personal Data in Optional Metadata Field**s: Customer should avoid submitting Personal Data in optional metadata fields (custom reference strings or job names) provided by the Services. These fields are intended solely for Customer's internal non-personal administrative references (e.g., batch identifiers, internal project codes).

If Customer submits Personal Data in such fields, Customer acknowledges that:

- Such data will be stored in Verifalia's database (not volatile RAM);
- Such data will be automatically deleted when the associated email addresses are deleted (upon expiry of the retention period or manual deletion by Customer);
- Anonymized job records (with Personal Data removed) will be retained for up to 2 years from the date of job creation for legitimate business purposes (billing verification, fraud prevention, service improvement, and analytics), after which they will be permanently deleted.

(b) Customer acknowledges that the Services are not designed or intended for the Processing of Prohibited Data as defined in subsection (a).

(c) Customer further acknowledges Section 12.2 of the Agreement, which provides that Customer must not rely on Verification Results for any purpose that could have a legal, financial, or material impact on any individual, including but not limited to decisions relating to credit, employment, education, housing, insurance, health, or legal matters.

4.3 Breach of Prohibited Data Restrictions

(a) If Verifalia becomes aware or reasonably suspects that Customer Data includes Prohibited Data in violation of Article 4.2, Verifalia may:

i. Immediately suspend Processing of the relevant Customer Data;

ii. Require Customer to immediately delete or remove such data from the Services;

iii. Delete such data from Verifalia's systems without further notice to Customer, where necessary to comply with Applicable Data Protection Laws or mitigate legal risk.

(b) Customer shall indemnify, defend, and hold harmless Verifalia from and against any and all claims, fines, penalties, damages, losses, costs, and expenses (including reasonable legal fees) arising from or relating to Customer's breach of Article 4.2, including any regulatory fines imposed on Verifalia as a result of Customer's submission of Prohibited Data.

4.4 Customer Warranty Regarding Marketing Use

(a) If Customer uses Verification Results for email marketing or commercial electronic communications, Customer represents and warrants that it will:

i. Comply with all applicable anti-spam, telemarketing, and marketing laws, including without limitation the EU e-Privacy Directive, GDPR consent requirements, US CAN-SPAM Act, Canada's Anti-Spam Legislation (CASL), and any other local laws in jurisdictions where recipients are located;

ii. Only send marketing emails to recipients who have provided valid, verifiable, and documented consent (where required by law);

iii. Provide a clear and functional unsubscribe mechanism in every marketing email and honor unsubscribe requests promptly;

iv. Include accurate sender identification and subject lines;

v. Not use Verification Results to send unsolicited bulk email, spam, or email in violation of applicable law.

(b) Customer acknowledges that Verifalia is not responsible for Customer's email marketing practices and that Customer is solely liable for any fines, penalties, or claims arising from Customer's violation of anti-spam laws.

(c) Customer shall indemnify Verifalia for any regulatory investigations, fines, penalties, or legal claims (including Data Subject claims or third-party claims) arising from Customer's violation of anti-spam laws.

For the avoidance of doubt, this indemnification does not extend to operational costs incurred by Verifalia in maintaining its infrastructure, IP reputation, or deliverability, which Verifalia assumes as part of providing the Services.

(d) **Verification is Not Consent**: Customer acknowledges that verification of an email address through the Services does not constitute evidence of consent to receive marketing communications. Customer must obtain consent independently in accordance with applicable law (e.g., GDPR Art. 6(1)(a), e-Privacy Directive Art. 13, CASL).

4.5 Protection of Service Integrity

(a) Customer acknowledges that Verifalia's Services rely on the reputation and deliverability of Verifalia's IP addresses and infrastructure.

(b) If Verifalia detects or receives complaints indicating that Customer's use of Verification Results may be causing reputational harm to Verifalia's infrastructure (such as IP blacklisting, spam complaints, or abuse reports), Verifalia will notify Customer and work cooperatively with Customer to investigate and resolve the issue.

(c) Verifalia reserves the right to take protective measures, including temporary throttling or rate limiting of Customer's verifications, or suspension or termination of Customer's Account, if necessary to protect the integrity of the Services for all customers.

5. PROCESSOR OBLIGATIONS

5.1 Confidentiality

(a) Verifalia shall ensure that all persons authorised to Process Customer Data (including Verifalia's employees, contractors, and Subprocessors) are subject to binding obligations of confidentiality (whether contractual or statutory) and have received appropriate training on data protection obligations.

(b) Verifalia shall ensure that such persons Process Customer Data only as necessary to provide the Services and in accordance with Customer's instructions and this DPA.

5.2 Cooperation and Assistance

Verifalia shall, taking into account the nature of the Processing and the information available to Verifalia, provide reasonable cooperation and assistance to Customer to enable Customer to comply with its obligations under Applicable Data Protection Laws, including:

(a) Assistance with Data Subject rights requests (Article 9);

(b) Assistance with data protection impact assessments and prior consultation with Supervisory Authorities (Article 10);

(c) Making available to Customer information necessary to demonstrate compliance with the obligations set forth in this DPA.

Upon reasonable request from Customer or a Supervisory Authority, Verifalia shall demonstrate compliance with its obligations under this DPA by providing:

- Records of Processing activities (Article 5.3);
- Evidence of technical and organizational measures (Annex 2);
- Copies of Subprocessor agreements or certifications of compliance;
- Audit reports or third-party certifications (subject to confidentiality);
- Records of Data Subject requests and responses;
- Incident logs and breach notifications.

(d) Cooperation with Customer and Supervisory Authorities in the event of investigations, audits, or enforcement actions relating to the Processing of Customer Data.

5.3 Records of Processing Activities

Verifalia shall maintain records of all categories of Processing activities carried out on behalf of Customer, in accordance with GDPR Article 30(2) or equivalent requirements under other Applicable Data Protection Laws. Such records shall include the information specified in Annex 1 and shall be made available to Customer or Supervisory Authorities upon reasonable request.

5.4 Compliance with Processor Obligations

Verifalia represents and warrants that it has implemented and will maintain appropriate policies, procedures, and controls to ensure compliance with all obligations applicable to Processors under Applicable Data Protection Laws, including GDPR Articles 28–36 and equivalent provisions under other data protection frameworks.

5.5 Cooperation with Supervisory Authorities

(a) Verifalia shall cooperate with Supervisory Authorities in accordance with GDPR Article 31 and equivalent provisions of other Applicable Data Protection Laws, but only with respect to matters within Verifalia's role and obligations as a Processor.

(b) Verifalia is not responsible for, and shall not be required to provide information regarding, Customer's compliance with Controller obligations under Applicable Data Protection Laws (including Customer's lawful basis for Processing, consent mechanisms, privacy notices, Data Subject rights fulfillment, or DPIAs).

(c) If a Supervisory Authority requests information from Verifalia regarding Customer's Controller obligations, Verifalia may refer the Supervisory Authority to Customer and shall notify Customer of such request (unless prohibited by law).

5.6 Limitations of Email Verification Technology

(a) Customer acknowledges that email verification is subject to technical and technological limitations inherent to the use of **artificial intelligence (AI)** and **machine learning (ML)** systems, and that Verification Results may not always be 100% accurate due to factors including but not limited to:

i. The probabilistic and continuously evolving nature of AI and ML algorithms;

ii. Limitations in AI/ML models' ability to accurately classify certain email patterns, domains, or mailbox configurations;

iii. Catch-all domains (domains configured to accept email for any address), which AI/ML systems may be unable to definitively verify due to technical limitations;

iv. Greylisting, rate limiting, and anti-spam measures implemented by recipient mail servers, which may interfere with AI/ML-based verification processes;

v. Temporary mail server outages or misconfigurations that may cause AI/ML systems to misclassify otherwise valid addresses;

vi. Privacy-protecting email services that block or obfuscate verification attempts, limiting AI/ML system accuracy;

vii. Changes in email address status between verification and actual email sending (e.g., mailbox full, account suspended, domain expired), which AI/ML models cannot predict;

viii. The inherent limitations of AI/ML systems in handling edge cases, novel patterns, or adversarial inputs not represented in training data.

These limitations are also disclosed in Section 12.2 of the Agreement, which Customer has acknowledged and accepted.

(b) Verifalia uses commercially reasonable efforts and industry-standard AI/ML techniques to provide accurate Verification Results and continuously improves its AI/ML models, but does not guarantee 100% accuracy or that emails sent to verified addresses will be delivered.

(c) Customer shall not rely exclusively on Verification Results for critical decisions and should implement additional safeguards (such as double opt-in mechanisms, bounce handling, and engagement tracking).

(d) Spam Traps and Honeypots: Certain email addresses are configured by ISPs, blacklist operators, or anti-spam organizations as "spam traps" to identify spammers. These addresses may appear syntactically valid and technically deliverable during verification. Verifalia's AI/ML models use commercially reasonable efforts to identify known spam traps, but cannot guarantee detection of all spam traps (particularly newly created or unlisted traps). Customer remains solely responsible for ensuring email addresses were legitimately obtained and that recipients have consented to receive email.

5.7 Fair Use and Rate Limits

Customer acknowledges and agrees that use of the Services is subject to:

(a) The Fair Use and Reasonable Use policy set forth in Section 10.3 of the Agreement; and

(b) API rate limits as specified in the Developer Documentation.

Verifalia may throttle, limit, or suspend Customer's access to the Services if Customer's usage is deemed excessive, abusive, or in violation of the Fair Use policy, as determined in Verifalia's sole discretion.

6. SUBPROCESSING

6.1 General Authorisation

(a) Customer provides general written authorisation for Verifalia to engage Subprocessors to Process Customer Data, provided that Verifalia complies with the requirements of this Article 6.

(b) A list of Subprocessors currently engaged by Verifalia, including their names, locations, and the services they provide, is set forth in Annex 3. **By accepting this DPA, Customer hereby authorizes Verifalia's engagement of the Subprocessors listed in Annex 3 as of the effective date of this DPA.**

(c) For any Subprocessors engaged after the effective date of this DPA, Verifalia shall comply with the notification and objection procedures set forth in Article 6.3.

6.2 Subprocessor Requirements

Verifalia shall:

(a) Enter into a written agreement with each Subprocessor imposing data protection obligations equivalent to those set forth in this DPA, including obligations regarding security, confidentiality, data subject rights, breach notification, international transfers, and deletion or return of Personal Data;

(b) Ensure that Subprocessors Process Customer Data only in accordance with Customer's instructions (as communicated through Verifalia) and Applicable Data Protection Laws;

(c) Remain fully liable to Customer for the performance of each Subprocessor's obligations, as required by GDPR Article 28(4).

(d) Ensure that any sub-processor agreement permits the Subprocessor to engage further sub-processors only with Verifalia's prior written authorization, and that equivalent data protection obligations are imposed on such further sub-processors.

6.3 Notification and Objection

(a) Verifalia shall notify Customer in writing (including by email to the preferred contact method associated with Customer's account administrators) of any intended addition or replacement of Subprocessors at least **thirty (30) calendar days** prior to authorising the new or replacement Subprocessor to access Customer Data.

(b) Such notification shall include:

i. The name and location of the proposed Subprocessor;

ii. A description of the Processing to be performed;

iii. Confirmation that a written agreement meeting the requirements of Article 6.2 will be in place.

(c) Customer may object to the engagement of a new or replacement Subprocessor on reasonable data protection grounds by notifying Verifalia in writing within thirty (30) calendar days of receipt of Verifalia's notification. Customer's objection shall specify the data protection grounds for the objection with reasonable particularity.

(d) If Customer validly objects to a new Subprocessor on reasonable data protection grounds:

i. Verifalia and Customer shall cooperate in good faith to resolve the objection, which may include Verifalia proposing alternative Subprocessors or additional safeguards;

ii. If the Parties cannot reach a mutually acceptable resolution within thirty (30) calendar days of Customer's objection, Customer may terminate the Agreement and this DPA by providing written notice to Verifalia, such termination to take effect before the new Subprocessor begins Processing Customer Data;

iii. Customer's right to terminate under this Article 6.3(d) is Customer's sole and exclusive remedy with respect to the engagement of a new or replacement Subprocessor to which Customer has validly objected.

(e) If Customer does not object within the thirty (30) day notice period, Customer shall be deemed to have accepted the new or replacement Subprocessor.

6.4 Subprocessor Changes to Annex 3

Verifalia may update Annex 3 from time to time to reflect additions, removals, or replacements of Subprocessors, provided that Verifalia complies with the notification and objection procedures set forth in Article 6.3. The current version of Annex 3 shall be made available to Customer via the Services or upon written request.

7. DATA SECURITY

7.1 Security Measures

(a) Verifalia has implemented and shall maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk of Processing Customer Data, taking into account:

- The state of the art;
- The costs of implementation;
- The nature, scope, context, and purposes of Processing;
- The risk of varying likelihood and severity for the rights and freedoms of natural persons.

(b) Such measures include those set forth in Annex 2 and shall include, as appropriate:

i. The pseudonymisation and encryption of Personal Data;

ii. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services;

iii. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

iv. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

(c) Verifalia shall ensure that Subprocessors implement security measures that meet or exceed the standards set forth in this Article 7 and Annex 2.

7.2 Privacy-by-Design and Privacy-by-Default

Verifalia has implemented privacy-by-design and privacy-by-default principles in accordance with GDPR Article 25, including:

- Volatile (RAM-only) storage of Personal Data, minimizing retention risk;
- Configurable data retention periods (5 minutes to 30 days), with automatic deletion upon expiry;
- Encryption of data in transit (TLS) and at rest (AES-256);
- Strict access controls and authentication mechanisms (MFA, RBAC, client certificate authentication);
- Prohibition of Special Categories of Personal Data through technical and contractual controls;

- Self-service data deletion functionality enabling Customer to delete data at any time;
- EU-only processing and storage (no third-country transfers except return to Customer).

These measures are described in detail in Annex 2 (Technical and Organisational Measures) and are regularly reviewed and updated to reflect evolving best practices and technological advancements.

7.3 Security Updates and Improvements

Verifalia shall regularly review and, where appropriate, update the technical and organisational measures described in Annex 2 to ensure ongoing compliance with Applicable Data Protection Laws and to address evolving security threats. Material changes to the security measures shall be communicated to Customer.

7.4 Security Assessments and Testing

Verifalia conducts regular security assessments, including:

(a) Periodic vulnerability assessments;

(b) Penetration testing by qualified third parties;

(c) Security monitoring and incident detection processes.

7.5 Customer Security Responsibilities

Customer is responsible for:

(a) Maintaining the security and confidentiality of Customer's account credentials (usernames, passwords, client certificates);

(b) Configuring appropriate security settings within the Services (such as multi-factor authentication, firewall settings, user permissions, and access controls);

(c) Ensuring that Customer's systems and networks used to access the Services are secure and do not introduce vulnerabilities;

(d) Promptly notifying Verifalia of any suspected or actual unauthorised access to Customer's account or Customer Data.

8. PERSONAL DATA BREACHES

8.1 Notification to Customer

(a) Verifalia shall notify Customer without undue delay, and in any event within **seventy-two (72) hours**, after becoming aware of a Personal Data Breach affecting Customer Data.

(b) Such notification shall be sent via email to the preferred contact method associated with Customer's account administrators and shall include, to the extent known at the time of notification:

i. A description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

ii. The likely consequences of the Personal Data Breach;

iii. A description of the measures taken or proposed to be taken by Verifalia to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;

iv. The name and contact details of Verifalia's data protection contact point or other designated contact from whom more information may be obtained.

(c) If it is not possible to provide all of the information specified in subsection (b) at the same time, Verifalia may provide the information in phases, without undue further delay, as the information becomes available.

8.2 Cooperation and Investigation

(a) Verifalia shall reasonably cooperate with Customer in investigating, mitigating, and remediating the Personal Data Breach, including:

i. Providing Customer with relevant details and documentation regarding the breach;

ii. Taking reasonable steps to mitigate the effects of the breach and prevent further unauthorised access or disclosure;

iii. Providing reasonable assistance to Customer in fulfilling Customer's obligations to notify Supervisory Authorities or Data Subjects, where required under Applicable Data Protection Laws.

(b) Customer shall be responsible for determining, in consultation with Verifalia as necessary, whether notification to Supervisory Authorities or Data Subjects is required under Applicable Data Protection Laws, and for making any such notifications.

(c) Customer acknowledges that certain jurisdictions impose stricter breach notification timelines or additional notification obligations beyond those in the GDPR, including but not limited to:

- **Australia**: Notification to the Office of the Australian Information Commissioner (OAIC) and affected individuals "as soon as practicable" (typically within 30 days);

- **Brazil**: Notification to the Autoridade Nacional de Proteção de Dados (ANPD) within a reasonable timeframe;
- **Singapore**: Notification to the Personal Data Protection Commission (PDPC) within 3 calendar days if the breach affects 500+ individuals or involves identity information;
- **South Africa**: Notification to the Information Regulator as soon as reasonably possible.
- **South Korea**: Notification to the Personal Information Protection Commission (PIPC) and affected individuals without undue delay;

Customer is solely responsible for determining whether such requirements apply to Customer and for making any required notifications to local authorities or Data Subjects within the required timeframes.

(d) Verifalia shall not inform any third party (including Data Subjects or Supervisory Authorities) of a Personal Data Breach without Customer's prior written consent, except where required by Applicable Data Protection Laws or by order of a court or regulatory authority, in which case Verifalia shall, to the extent legally permitted, provide Customer with prior notice of such disclosure.

8.3 Breach Prevention and Remediation

Following a Personal Data Breach, Verifalia shall take appropriate measures to prevent recurrence, which may include:

(a) Conducting a root cause analysis;

(b) Implementing additional security controls;

(c) Enhancing monitoring and detection capabilities;

(d) Providing training to personnel;

(e) Reviewing and updating Subprocessor agreements and security requirements.

8.4 Subprocessor Breach Notification

Verifalia shall ensure that all Subprocessor agreements require Subprocessors to notify Verifalia without undue delay upon becoming aware of any Personal Data Breach affecting Customer Data. Verifalia shall then notify Customer in accordance with Article 8.1.

8.5 Government Access Requests (Transparency Clause)

(a) If Verifalia receives a legally binding request from a government authority, law enforcement agency, or court for access to or disclosure of Customer Data, Verifalia shall:

i. Notify Customer of such request without undue delay, unless prohibited by law;

ii. Provide Customer with a copy of the request (if legally permissible);

iii. Challenge the request if Verifalia has reasonable grounds to believe it is unlawful or overly broad;

iv. Cooperate with Customer in seeking protective orders or other relief.

(b) Verifalia shall disclose only the minimum Customer Data necessary to comply with the legally binding request and shall request confidential treatment of any disclosed data.

9. DATA SUBJECT RIGHTS

9.1 Data Subject Requests

(a) **Direct Requests to Customer**: Data Subjects shall exercise their rights under Applicable Data Protection Laws (including rights of access, rectification, erasure, restriction, data portability, objection, and rights relating to automated decision-making) by contacting Customer directly. Verifalia shall not respond to Data Subject requests directly without Customer's prior written authorization.

(b) **Requests Received by Verifalia**: If Verifalia receives a Data Subject request relating to Customer Data (whether by email, written correspondence, or other means), Verifalia shall:

i. **Provide a standard response** to the Data Subject (if contact information is provided) informing the Data Subject that:

- Verifalia acts as a data processor on behalf of multiple data controllers;
- Due to Verifalia's technical architecture (volatile storage, multi-customer processing, and data minimization practices), Verifalia cannot identify which controller(s) processed the Data Subject's Personal Data or associate the Data Subject's email address with a specific controller;
- The Data Subject should contact directly the organization(s) from which the Data Subject received communications, with which the Data Subject has a business relationship, or to which the Data Subject provided their email address, as such organization(s) are the responsible data controller(s);
- Verifalia cannot forward the Data Subject's request to a specific controller without information that would enable Verifalia to identify the relevant controller (such as the controller's name or other identifying details provided by the Data Subject).

ii. **Not respond substantively** to the Data Subject request or access, retrieve, or process Customer Data in response to the request, except as described in

subsection (b)(i) above or unless otherwise instructed in writing by a Customer who confirms the request relates to that Customer's Processing activities.

(c) **Technical Limitations - Processor Architecture**: Customer acknowledges that Verifalia's data processing architecture is designed to:

i. Minimize data retention through volatile (RAM-only) storage;

ii. Serve multiple Controllers who may submit overlapping or identical email addresses;

iii. Automatically and permanently delete Personal Data upon expiry of configurable retention periods;

iv. Maintain no persistent or easily accessible linkage between specific email addresses and Customer account identities, as a privacy-enhancing technical measure.

As a result of this architecture, Verifalia cannot systematically identify which Controller(s) submitted a particular email address for verification, particularly after such data has been deleted. This design is implemented as a privacy-enhancing measure in accordance with GDPR Article 25 (data protection by design and by default).

(d) **Customer's Responsibility**: Customer, as the Controller with a direct relationship with Data Subjects, is solely responsible for:

i. Implementing mechanisms to receive and respond to Data Subject requests directly;

ii. Providing clear privacy notices to Data Subjects identifying Customer as the Controller and providing Customer's contact information for rights requests;

iii. Maintaining records enabling Customer to identify whether specific Personal Data has been processed by Customer through the Services;

iv. Fulfilling Data Subject requests within the timelines required by Applicable Data Protection Laws.

(e) **Notification to Customer - Optional Cooperation**: If a Data Subject provides sufficient information in their request to Verifalia that would enable identification of a specific Customer (such as explicitly naming the Customer, providing an account reference, or describing circumstances that clearly identify a particular Customer), and if Verifalia is able to identify the relevant Customer based on such information, Verifalia may, at its discretion, notify such Customer of the Data Subject request to facilitate Customer's response. However, Verifalia is under no obligation to conduct investigations, searches, or analysis to identify the relevant Customer, and the absence of such notification does not constitute a breach of this DPA.

9.2 Customer Self-Service Capabilities

(a) Customer acknowledges that the Services provide Customer with the ability to independently fulfill most Data Subject requests through the functionality of the Services, including:

i. **Access and Data Portability**: Customer may access and export Verification Results at any time via the Services in machine-readable formats (JSON, CSV, Excel);

ii. **Erasure**: Customer may delete Verification Results at any time via the Services by using the deletion functionality or by configuring shorter data retention periods. Upon deletion, Customer Data is immediately and permanently destroyed and cannot be recovered.

(b) Given the volatile nature of Verifalia's data storage architecture (RAM-only, temporary storage with configurable retention periods between 5 minutes and 30 days), and Customer's self-service capabilities, Verifalia anticipates that most Data Subject requests can be fulfilled by Customer without requiring Verifalia's assistance.

9.3 Assistance with Data Subject Requests

(a) To the extent Customer is unable to independently fulfill a Data Subject request using the functionality of the Services, Customer may request Verifalia's assistance by submitting a support request through the **"Request support" feature** available in the Verifalia application at https://app.verifalia.com

(b) Verifalia shall provide assistance taking into account the nature and complexity of the request. Verifalia shall respond to requests for assistance without undue delay.

(c) Customer acknowledges and agrees that:

i. i. Once Customer Data is deleted (whether by Customer via the Services, automatically upon expiry of the configured retention period, or upon termination of the Agreement), the data is immediately and permanently destroyed from Verifalia's systems and cannot be recovered or restored;

ii. ii. Verifalia cannot fulfill Data Subject requests (such as access or data portability) for Customer Data that has already been deleted.

(d) **Record Keeping**: Verifalia shall maintain a log of Data Subject requests received pursuant to Article 9.1(b), including date received, nature of request, and date Customer was notified. Such log shall be retained for three (3) years and made available to Customer or Supervisory Authorities upon request for compliance verification purposes.

(e) **Alternative Contact Method**: If Customer is unable to access the in-app support feature due to technical issues or account access problems, Customer may contact support@verifalia.com, providing sufficient information to verify Customer's identity and account ownership. Verifalia reserves the right to authenticate Customer's identity before providing assistance through alternative channels.

9.4 Costs of Assistance

(a) **Tier 1 Assistance (Standard Responses to Data Subjects)**: Verifalia shall provide the standard response to Data Subjects as described in Article 9.1(b)(i) at no additional charge. This includes:

i. Acknowledging receipt of the Data Subject request;

ii. Informing the Data Subject that Verifalia acts as a Processor and cannot identify the relevant Controller;

iii. Directing the Data Subject to contact the appropriate Controller(s);

(b) **Tier 2 Assistance (Complex or High-Volume Requests)**: If a Data Subject request or series of requests requires significant manual effort, custom development, forensic analysis, or Verifalia personnel time exceeding **four (4) hours** in any thirty (30) day period (including but not limited to manual searches across systems, technical investigations to identify whether specific data was processed, or responding to multiple related requests from the same Data Subject), Verifalia may charge Customer for such assistance at Verifalia's then-current professional services rates. Verifalia shall notify Customer of anticipated charges and obtain Customer's approval before incurring such costs.

(c) **Customer-Borne Costs**: All costs associated with fulfilling Data Subject requests, including any fees charged by Verifalia under subsection (b), shall be borne exclusively by Customer.

10. DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

10.1 Assistance with DPIAs

To the extent required by Applicable Data Protection Laws (including GDPR Article 35), Verifalia shall provide reasonable assistance to Customer in conducting data protection impact assessments ("**DPIAs**") relating to Customer's use of the Services, taking into account the nature of the Processing and the information available to Verifalia.

10.2 Information for DPIAs

Upon Customer's written request, Verifalia shall provide Customer with relevant information regarding Verifalia's Processing of Customer Data, including:

(a) The details of Processing set forth in Annex 1;

(b) The technical and organisational measures set forth in Annex 2;

(c) The Subprocessors listed in Annex 3 and the safeguards applied to Subprocessing;

(d) The measures Verifalia has implemented to ensure security and mitigate risks, as described in Article 7 and Annex 2.

10.3 Prior Consultation

If Customer is required to consult with a Supervisory Authority under GDPR Article 36 or equivalent provisions of other Applicable Data Protection Laws, Verifalia shall, upon request, provide Customer with reasonable assistance and cooperation, including providing information necessary for such consultation.

10.4 Costs of Assistance

(a) Verifalia shall provide assistance under this Article 10 at no additional charge where such assistance can be provided through standard operational processes and does not require extraordinary effort.

(b) If assistance requires significant manual effort, custom analysis, or Verifalia personnel time exceeding four (4) hours, Verifalia may charge Customer at Verifalia's then-current professional services rates. Verifalia shall notify Customer of anticipated charges and obtain Customer's approval before incurring such costs.

(c) All costs associated with DPIAs and prior consultation, including any fees charged by Verifalia, shall be borne exclusively by Customer.

11. DELETION AND RETURN OF PERSONAL DATA

11.1 Data Retention During Agreement Term

Verifalia shall retain Customer Data in accordance with the following tiered retention framework:

(a) **Primary Customer Data (Email Addresses and Verification Results)**: Email addresses, verification metadata, and custom reference strings submitted by Customer are stored in volatile (RAM-only) memory and automatically deleted upon expiry of the retention period configured by Customer. Customer may configure retention periods between 5 minutes and 30 days per verification job. Upon expiry, all data stored in volatile memory is permanently and irreversibly deleted.

(b) **Incidental Personal Data (Optional Metadata Fields and IP Addresses)**: To the extent Customer submits Personal Data in optional metadata fields (custom reference strings, job names), or when Customer's IP address is collected during job submission, such

data is automatically deleted at the same time email addresses are deleted (subsection (a) above). Deletion replaces Personal Data with the following values:

- Custom reference strings and Job names: automatically deleted (set to null)
- IP addresses: Replaced with the anonymized placeholder "0.0.0.0".

(c) **Anonymized Job Records**: After deletion of Personal Data (subsections (a)-(b) above), job records containing non-personal metadata (including job ID, quality settings, priority settings, timestamps, and anonymized IP addresses) are retained for up to 2 years from the date of job creation for the following legitimate business purposes:

- Customer analytics and service improvement (aggregate usage patterns, performance optimization);
- Billing verification and audit trail (proof of services rendered);
- Fraud prevention and abuse detection (identification of suspicious patterns).

These anonymized records constitute truly anonymous data that do not constitute Personal Data under GDPR Article 4(1) and Recital 26, as they do not relate to identified or identifiable natural persons and cannot be re-identified using reasonable means. The retention of such anonymized data is based on Verifalia's legitimate interests pursuant to GDPR Article 6(1)(f), and such interests have been assessed as not being overridden by the interests or fundamental rights and freedoms of Data Subjects, given that the data has been fully anonymized.

Timestamps are retained at full granularity for analytical and billing purposes. Given the volume of verification jobs processed across all customers, timestamps combined with anonymized data (job ID, anonymized IP address) do not enable re-identification of individual Customers or Data Subjects and therefore do not constitute Personal Data.

(d) **Final Deletion**: All anonymized job records are permanently deleted from Verifalia's systems 2 years after the date of job creation. No data (personal or anonymized) related to the verification job is retained beyond this period.

(e) **Manual Deletion by Customer**: If Customer manually deletes a verification job before the configured retention period expires, the deletion process follows the same deletion and anonymization procedure as automatic expiry (subsections (a)-(d) above). Email addresses, custom reference strings and job names are immediately deleted, and IP addresses are immediately anonymized in the database.

(f) **Account Deletion**: If Customer deletes their Verifalia account, all active verification jobs (those still within their configured retention periods) are immediately processed as described in subsection (e) above (email addresses deleted, metadata deleted or anonymized). Anonymized job records associated with the deleted account are retained for up to 2 years from their original creation dates (subsection (c) above) for billing, legal compliance, and fraud prevention purposes, after which they are permanently deleted.

11.2 Deletion Upon Termination

(a) Upon termination or expiration of the Agreement for any reason, Verifalia will delete all Customer Data in Verifalia's possession or control in accordance with Article 11.1.

(b) Deletion under this Article 11.2 shall be completed within thirty (30) calendar days following the effective date of termination, except to the extent retention is required by Applicable Data Protection Laws or other legal obligations.

11.3 Certification of Deletion

Upon written request from Customer, Verifalia shall provide written certification that Customer Data has been deleted in accordance with this Article 11.

11.4 Subprocessor Deletion

Verifalia shall ensure that all Subprocessors delete or return Customer Data in accordance with this Article 11 and in compliance with the terms of the Subprocessor agreements.

12. AUDIT RIGHTS

12.1 Customer Audit Rights

Customer has the right to verify Verifalia's compliance with this DPA through the audit mechanisms set forth in this Article 12. Customer shall exercise such audit rights in a manner that does not unreasonably interfere with Verifalia's business operations.

12.2 Tier 1: Documentation Review

(a) Upon reasonable written request from Customer (and no more than once per twelve (12) month period, unless a Personal Data Breach has occurred or a Supervisory Authority requires more frequent audits), Verifalia shall provide Customer with:

i. Copies of Verifalia's current information security policies and procedures (subject to redaction of commercially sensitive or proprietary information);

ii. Copies of executed Subprocessor agreements (redacted to remove commercially sensitive terms), or certifications that such agreements contain the required data protection provisions;

iii. Evidence of the technical and organisational measures implemented by Verifalia as described in Annex 2;

iv. Any audit reports or certifications issued to Verifalia by its Subprocessors (e.g., Hetzner, AWS), to the extent such reports are available to Verifalia and not subject to confidentiality restrictions.

v. Copies of any third-party security certifications held by Verifalia (such as ISO 27001, SOC 2, or equivalent), to the extent such certifications exist and are not subject to confidentiality restrictions.

(b) Verifalia shall respond to requests under this Article 12.2 within thirty (30) calendar days of receipt.

12.3 Tier 2: Additional documentation and custom requests

(a) If the documentation provided under Article 12.2 is insufficient to verify compliance with this DPA, and subject to the restrictions in subsection (c), Customer may request additional documentation to assess Verifalia's compliance by submitting additional security questionnaires or information requests to Verifalia.

(b) Such requests are limited to one (1) written questionnaire or information request per twelve (12) month period, unless a Personal Data Breach has occurred affecting Customer Data or a Supervisory Authority or regulatory body requires an additional assessment.

(c) **Costs**: Customer shall bear all costs associated with remote assessments, including:

i. Customer's own personnel time, consultants, and legal advisors;

ii. Verifalia's personnel time to the extent such time exceeds two (2) hours per assessment, charged at Verifalia's then-current professional services rates: Verifalia shall notify Customer if an assessment is anticipated to exceed two (2) hours and obtain Customer's approval before incurring such charges.

12.4 Tier 3: On-Site Audits

(a) Customer may conduct an on-site audit of Verifalia's facilities **only** in the following exceptional circumstances:

i. A serious Personal Data Breach has occurred that affects Customer Data, **and** the documentary audit methods set forth in Articles 12.2–12.3 are insufficient to verify Verifalia's compliance or investigate the breach; **or**

ii. A Supervisory Authority or regulatory body with jurisdiction over Customer has issued a formal request or order requiring an on-site audit of Verifalia; **or**

iii. Customer has reasonable, documented evidence (not mere suspicion) that Verifalia has materially breached its obligations under this DPA, and such breach cannot be adequately investigated through remote methods.

(b) **Scope and Location**: On-site audits shall be conducted in Padova, Italy. Customer acknowledges that Verifalia does not own or operate data centers and relies on Subprocessor infrastructure; accordingly, on-site audits shall not include access to Subprocessor facilities (which are subject to the Subprocessors' own audit rights and physical security policies).

(c) **Advance Notice and Scheduling**: Customer shall provide Verifalia with at least **sixty (60) calendar days'** advance written notice of any proposed on-site audit. The audit shall be scheduled at a mutually agreeable time during Verifalia's regular business hours and shall be conducted in a manner that does not unreasonably disrupt Verifalia's operations.

(d) Audit Scope and Conduct:

i. The audit shall be conducted by qualified auditors or information security professionals engaged by Customer (not Customer's employees, unless such employees hold relevant professional certifications such as CISM, CISSP, or equivalent);

ii. All auditors shall execute Verifalia's standard confidentiality and non-disclosure agreement prior to the audit;

iii. The audit shall be limited in scope to verifying Verifalia's compliance with the specific obligations set forth in this DPA and shall not extend to unrelated business operations, customer data of other customers, or proprietary systems and methodologies;

iv. Verifalia may require that a Verifalia representative be present at all times during the audit.

(e) **Audit Report**: Customer shall provide Verifalia with a copy of the final audit report within thirty (30) calendar days following completion of the audit. The report shall include findings, recommendations, and any identified non-compliance with this DPA. Verifalia shall have thirty (30) calendar days to respond to the audit report and, if applicable, propose a remediation plan.

(f) **Costs:** All costs associated with on-site audits shall be borne exclusively by Customer, including without limitation:

i. Travel, accommodation, and expenses of Customer's auditors;

ii. Verifalia's personnel time required to support the audit, charged at Verifalia's then-current professional services rates;

iii. Any third-party costs incurred by Verifalia in connection with the audit (such as legal review, data room setup, or document preparation).

Verifalia shall provide Customer with a cost estimate prior to the audit, and Customer shall approve such costs in writing before the audit commences.

12.5 Cooperation with Supervisory Authorities

Notwithstanding the audit rights set forth in this Article 12, Verifalia shall allow for and contribute to audits, including inspections, conducted by Supervisory Authorities or auditors mandated by Supervisory Authorities, in accordance with Applicable Data Protection Laws.

12.6 Limitations on Audit Rights

(a) Audit rights under this Article 12 do not entitle Customer to:

i. Access Personal Data of other customers or Data Subjects unrelated to Customer;

ii. Access Verifalia's proprietary systems, source code, algorithms, trade secrets, or confidential business information unrelated to the Processing of Customer Data or compliance with this DPA;

iii. Disrupt Verifalia's operations or those of other customers.

(b) Customer shall treat all information obtained during an audit as Verifalia's Confidential Information and shall use such information solely for the purpose of verifying compliance with this DPA.

13. INTERNATIONAL DATA TRANSFERS

13.1 Processing Location

(a) Verifalia Processes all Customer Data within the **European Economic Area (EEA)**, specifically in **Germany**.

(b) All Subprocessors engaged by Verifalia to Process Customer Data are located within the EEA (Germany), as set forth in Annex 3.

(c) Verifalia does not transfer Customer Data outside the EEA, except as expressly set forth in this Article 13.

13.2 Transfers to Customer

(a) **Return of Data:** When Customer accesses or downloads Verification Results (Customer Data) through the Services, such access or download may constitute a Restricted Transfer if Customer is located outside the EEA, United Kingdom, or Switzerland.

(b) **Customer as Data Importer:** For such Restricted Transfers, Customer acts as the data importer and is responsible for ensuring that it has an appropriate legal basis and safeguards under Applicable Data Protection Laws for receiving the Customer Data.

(c) Customer warrants that it will comply with all Applicable Data Protection Laws in its jurisdiction with respect to the receipt and subsequent Processing of Customer Data returned by Verifalia.

13.3 Standard Contractual Clauses for Restricted Transfers

(a) To the extent that Verifalia Processes Customer Data subject to the GDPR or UK GDPR and such Processing involves or is reasonably likely to involve a Restricted Transfer (including transfers to Customer located outside the EEA or UK), the Parties hereby incorporate by reference and agree to comply with the **Standard Contractual Clauses** set forth in Annex 4, which shall form an integral part of this DPA.

(b) The specifications, module selection, party designations, and other details of the Standard Contractual Clauses are set forth in Annex 4.

(c) For transfers subject to the **UK GDPR**, the UK International Data Transfer Addendum (version B1.0 or as updated) to the EU Standard Contractual Clauses applies, with the above specifications adapted as necessary for UK law.

13.4 Transfer Impact Assessments

(a) Given that all Processing occurs within the EEA (Germany) and Verifalia does not transfer Customer Data to third countries outside the EEA (except for return to Customer), Verifalia does not routinely conduct Transfer Impact Assessments ("**TIAs**") under the Schrems II framework.

(b) If Customer reasonably believes that a TIA is required due to changes in circumstances (such as changes in third-country laws applicable to Customer or requests by Customer's Supervisory Authority), Customer may request that Verifalia provide information to assist Customer in conducting such TIA. Verifalia shall provide reasonable cooperation, subject to Article 10.4 (cost of assistance).

13.5 Additional Safeguards

In accordance with the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Verifalia implements the following supplementary measures to ensure the protection of Customer Data:

(a) **Encryption**: Customer Data is encrypted in transit (TLS) and at rest (AES-256);

(b) **Volatile Storage**: Customer Data is stored only in RAM (non-persistent memory) and is automatically deleted upon expiry of the configured retention period;

(c) **Access Controls**: Strict access controls and authentication mechanisms (MFA, RBAC, client certificate authentication, configurable firewall settings) limit access to Customer Data;

(d) **EEA-Only Processing**: All Processing, storage, and Subprocessing occur exclusively within the EEA;

(e) **No Third-Country Access**: Verifalia does not have remote personnel or service providers outside the EEA with access to Customer Data.

13.6 Customer Obligations for Third-Country Transfers

If Customer is located outside the EEA, United Kingdom, or Switzerland, or if Customer subsequently transfers Customer Data received from Verifalia to a third country, Customer is solely responsible for:

(a) Ensuring compliance with Applicable Data Protection Laws in Customer's jurisdiction;

(b) Implementing appropriate safeguards for such transfers (such as Standard Contractual Clauses, Binding Corporate Rules, adequacy decisions, or derogations);

(c) Conducting any required Transfer Impact Assessments;

(d) Obtaining any required authorizations from Supervisory Authorities.

14. LIABILITY AND INDEMNIFICATION

14.1 Allocation of Liability for Data Protection Violations

14.1.1 Regulatory Fines

Each Party shall be liable for regulatory fines and penalties (including fines imposed under GDPR Article 83 or equivalent provisions of other Applicable Data Protection Laws) as follows:

(a) **Verifalia's Liability**: Verifalia shall be solely liable for fines and penalties imposed on Verifalia as a result of Verifalia's failure to:

- Comply with its obligations as a Processor under this DPA or Applicable Data Protection Laws;
- Process Customer Data in accordance with Customer's lawful instructions;
- Implement appropriate technical and organisational measures;
- Ensure Subprocessor compliance;
- Notify Customer of Personal Data Breaches; or
- Otherwise fulfill Processor obligations under GDPR Articles 28–36 or equivalent provisions.

(b) **Customer's Liability**: Customer shall be solely liable for fines and penalties imposed on Customer as a result of Customer's failure to:

- Establish a lawful basis for Processing under Applicable Data Protection Laws;
- Provide lawful instructions for Processing;
- Comply with Controller obligations under Applicable Data Protection Laws;
- Obtain necessary consents, authorizations, or provide required notices to Data Subjects;
- Submit only lawful and authorized Personal Data to the Services (including the prohibition on Prohibited Data under Article 4.2);
- Notify Data Subjects or Supervisory Authorities of Personal Data Breaches where required; or
- Otherwise fulfill Controller obligations.

(c) **Joint Liability**: If a regulatory fine or penalty is imposed jointly on both Parties, or if it is not possible to clearly allocate fault to one Party:

i. The Parties shall cooperate in good faith to determine each Party's proportionate degree of responsibility for the infringement giving rise to the fine;

ii. Liability shall be apportioned according to each Party's degree of responsibility, as determined by the Supervisory Authority, court, or arbitrator, or as mutually agreed by the Parties;

This allocation is in accordance with GDPR Article 82(4) and (5), which establish joint and several liability and the right of full recovery between controllers and processors.

(d) **Right of Recovery**: If one Party pays a fine or penalty for which the other Party is wholly or partially responsible under this Article 14.1.1, the paying Party shall have a right of recovery against the responsible Party for the portion of the fine attributable to such Party's fault.

14.1.2 Data Subject Compensation Claims

(a) **GDPR Article 82 Compliance**: Each Party acknowledges that under GDPR Article 82 and equivalent provisions of other Applicable Data Protection Laws, Data Subjects have the right to receive compensation for material or non-material damage resulting from infringements of data protection law.

(b) **Allocation of Liability to Data Subjects**:

i. Where a Data Subject suffers damage and brings a claim for compensation against either Party, the Parties agree to allocate liability as follows:

- **Verifalia is liable** for damage caused by Verifalia's infringement of data protection obligations specifically directed to Processors under Applicable Data Protection Laws, or by Processing outside or contrary to Customer's lawful instructions;
- **Customer is liable** for damage caused by Customer's infringement of Controller obligations under Applicable Data Protection Laws, including failure to establish lawful basis for Processing, unlawful Processing instructions, or submission of Prohibited Data;
- **Joint and several liability** applies if both Parties contributed to the same damage. Each Party is liable to the Data Subject for the full amount of the damage, but may seek contribution or indemnification from the other Party in accordance with subsection (c).

ii. A Party shall be exempted from liability under this Article 14.1.2 if it proves that it is not in any way responsible for the event giving rise to the damage (GDPR Article 82(3)).

(c) Right of Recovery Between Parties:

i. If one Party compensates a Data Subject for damage caused wholly or in part by the other Party's infringement of this DPA or Applicable Data Protection Laws, the compensating Party shall have a right of full recovery against the responsible Party, to the extent the damage was caused by such Party's infringement;

ii. If both Parties contributed to the damage, the right of recovery shall be proportionate to each Party's degree of fault;

iii. The Parties shall reasonably cooperate in defending against Data Subject claims and in apportioning liability.

(d) **No Limitation of Data Subject Rights**: Nothing in this DPA limits or restricts the rights of Data Subjects to bring claims or seek compensation under Applicable Data Protection Laws. Any limitations of liability in this Article 14 apply solely to the allocation of liability between the Parties and do not affect Data Subjects' rights.

14.2 Limitation of Liability Between Parties

14.2.1 Bifurcated Liability Caps

(a) **For breaches of this DPA that do not involve Personal Data Breaches or violations of Applicable Data Protection Laws:**

The liability cap set forth in Section 13.2 of the Agreement applies: Verifalia's total aggregate liability shall not exceed the lesser of:

i. the total Subscription Charges paid by Customer to Verifalia during the **one (1) month period** immediately preceding the event giving rise to liability, **or**

ii. **EUR 100 (one hundred euros)**.

(b) **For Personal Data Breaches or violations of Applicable Data Protection Laws**:

Verifalia's total aggregate liability to Customer (excluding regulatory fines and Data Subject compensation claims, which are governed by Article 14.1) shall not exceed the **lesser of**:

i. The total Subscription Charges paid by Customer to Verifalia during the **six (6) months** immediately preceding the event giving rise to liability; **or**

ii. **EUR 1,000 (one thousand euros)**.

(c) Exclusions from Liability Caps:

The limitations set forth in subsections (a) and (b) do not apply to:

i. Verifalia's gross negligence or willful misconduct;

ii. Fraud;

iii. Breach of confidentiality obligations under Article 5.1;

iv. Regulatory fines and penalties (governed by Article 14.1.1);

v. Data Subject compensation claims (governed by Article 14.1.2);

vi. Liabilities that cannot be limited or excluded under Applicable Data Protection Laws or other mandatory laws;

vii. Death or personal injury caused by Verifalia's negligence.

14.2.2 Exclusion of Consequential Damages

To the maximum extent permitted by applicable law, in no event shall either Party be liable to the other for any indirect, incidental, special, consequential, exemplary, or punitive damages (including loss of profits, revenue, business opportunities, goodwill, anticipated savings, or data) arising out of or related to this DPA, regardless of the theory of liability (contract, tort, negligence, strict liability, or otherwise), and even if such Party has been advised of the possibility of such damages.

This exclusion does not apply to:

(a) Regulatory fines and Data Subject compensation claims (which are direct, not consequential, damages under data protection law);

(b) Liabilities arising from gross negligence, willful misconduct, or fraud;

(c) Liabilities that cannot be excluded under Applicable Data Protection Laws or other mandatory laws.

14.3 Customer Indemnification Obligations

Customer shall indemnify, defend, and hold harmless Verifalia and its affiliates, and their respective directors, officers, employees, agents, contractors, and Subprocessors (collectively, the "**Verifalia Indemnified Parties**") from and against any and all claims, liabilities, damages, losses, costs, and expenses (including reasonable legal fees and costs of investigation and defense) arising out of or related to:

(a) Customer's breach of this DPA, including breach of Article 4 (Customer Instructions and Prohibited Data);

(b) Customer's violation of Applicable Data Protection Laws in its capacity as Controller, including failure to establish lawful basis for Processing, failure to obtain required consents, or failure to provide required notices;

(c) Customer's submission of Prohibited Data to the Services in violation of Article 4.2;

(d) Any claim by a Data Subject, Supervisory Authority, or third party alleging that Customer Data or Customer's use of the Services infringes or violates any third party's rights (including intellectual property, privacy, or publicity rights) or applicable law;

(e) Any regulatory investigation, enforcement action, or fine imposed on Verifalia as a result of Customer's unlawful instructions or violation of Controller obligations;

(f) Customer's use of the Services in a manner not authorized by this DPA or the Agreement;

(g) Customer's violation of anti-spam laws, anti-fraud laws, or marketing regulations in connection with the use of Verification Results, as contemplated by Section 6.4 of the Agreement;

(h) Any breach of Customer's warranties and representations under Articles 3.1 or 4.2.

14.4 Indemnification Procedure

(a) Verifalia will:

i. Provide Customer with prompt written notice of any claim subject to Customer's indemnification obligations under Article 14.3 (provided that failure to provide prompt notice shall not relieve Customer of its indemnification obligations except to the extent Customer is materially prejudiced thereby);

ii. Allow Customer to control the defense and settlement of such claim, provided that Customer may not settle any claim in a manner that imposes any obligation or liability on Verifalia, admits fault on behalf of Verifalia, or requires Verifalia to pay

any amount, without Verifalia's prior written consent (not to be unreasonably withheld);

iii. Provide reasonable cooperation in the defense of such claim, at Customer's expense.

(b) Notwithstanding subsection (a)(ii), Verifalia reserves the right, at its own expense, to participate in the defense of any claim subject to Customer's indemnification obligations using counsel of Verifalia's choice.

14.5 Survival

The provisions of this Article 14 shall survive the termination or expiration of this DPA and the Agreement.

15. TERM AND TERMINATION

15.1 Term

This DPA shall commence on the date Customer first accesses or uses the Services and shall continue in full force and effect for so long as Verifalia Processes Customer Data on behalf of Customer, unless earlier terminated in accordance with this Article 15.

15.2 Termination in Connection with Agreement

(a) This DPA shall automatically terminate upon the termination or expiration of the Agreement for any reason, subject to Article 15.4 (Survival).

(b) Customer may terminate the Agreement (and thereby this DPA) at any time in accordance with Section 15.1 of the Agreement (by requesting account closure).

(c) Verifalia may terminate or suspend Customer's access to the Services (and thereby terminate or suspend this DPA) in accordance with Section 15.2 of the Agreement, including for Customer's breach of this DPA.

15.3 Termination for Material Breach of DPA

(a) Either Party may terminate this DPA (and the Agreement) immediately upon written notice if the other Party:

i. Materially breaches this DPA and fails to cure such breach within **thirty (30) calendar days** following receipt of written notice specifying the breach; **or**

ii. Commits a breach of this DPA that is incapable of cure (such as unauthorized disclosure of Customer Data to third parties or Processing Customer Data for purposes other than providing the Services).

(b) Customer may terminate this DPA immediately upon written notice if:

i. Verifalia fails to comply with a Supervisory Authority order or legally binding decision relating to Customer Data and such failure materially affects Customer's rights or obligations under Applicable Data Protection Laws; **or**

ii. A Supervisory Authority or court determines that Verifalia's Processing of Customer Data violates Applicable Data Protection Laws, and Verifalia fails to remedy such violation within a reasonable period.

15.4 Effect of Termination; Survival

(a) Upon termination or expiration of this DPA for any reason:

i. Verifalia shall cease all Processing of Customer Data, except as necessary to comply with Article 11 (Deletion and Return of Personal Data) or as required by Applicable Data Protection Laws;

ii. Verifalia shall delete Customer Data in accordance with Article 11;

iii. Customer remains liable for all fees and charges incurred prior to the effective date of termination;

iv. Any unused Credit Pack balances (including credits purchased via Auto Top-Up) and unused paid subscription periods are forfeited and non-refundable, except as required by mandatory consumer protection laws.

(b) Survival: The following provisions shall survive termination or expiration of this DPA:

- Article 1 (Definitions and Interpretation)
- Article 5.1 (Confidentiality)
- Article 7.5 (Customer Security Responsibilities)
- Article 11 (Deletion and Return of Personal Data)
- Article 12 (Audit Rights) – to the extent necessary to verify post-termination compliance
- Article 14 (Liability and Indemnification)
- Article 16.3 (Confidentiality)
- Article 16.7 (Governing Law and Dispute Resolution)
- Article 16.8 (Notices)

- Any other provisions that by their nature are intended to survive

(c) This DPA shall remain in effect until the later of:

i. Completion of all obligations under Article 11 (Deletion of Personal Data); or

ii. Thirty (30) calendar days following the effective date of termination of the Agreement.

16. GENERAL PROVISIONS

16.1 Relationship to Agreement

(a) This DPA is incorporated into and forms part of the Agreement. Except as expressly set forth in this DPA, all terms and conditions of the Agreement remain in full force and effect.

(b) In the event of any conflict or inconsistency between the provisions of the Agreement and this DPA with respect to the Processing of Customer Data or compliance with Applicable Data Protection Laws, this DPA shall prevail.

(c) For the avoidance of doubt, this DPA does not replace, modify, or supersede the Agreement with respect to matters not related to data protection (such as licensing, fees, payment terms, warranties unrelated to data protection, or general commercial terms).

16.2 Amendments

(a) **Material Amendments**: Verifalia may amend this DPA from time to time to reflect:

i. Changes in Applicable Data Protection Laws or guidance from Supervisory Authorities;

ii. Changes to Verifalia's data processing practices, security measures, or Subprocessors (subject to Article 6.3);

iii. Clarifications, corrections, or improvements to this DPA.

(b) **Notice of Material Amendments**:

i. Verifalia shall notify Customer of any material amendments to this DPA by:

- Updating the "Last updated" date at the top of this document;
- Sending email notification to the preferred contact methods associated with Customer's account administrators; and/or

- Posting a prominent notice on the Services or Verifalia's website.

ii. Such notice shall be provided at least **thirty (30) calendar days** prior to the effective date of the amendment, except where amendments are required by law or regulatory order, in which case they may take effect immediately upon notice.

(c) **Customer's Right to Object**:

i. If Customer reasonably objects to a material amendment on data protection grounds, Customer may terminate the Agreement and this DPA by providing written notice to Verifalia within the thirty (30) day notice period, such termination to take effect before the amendment becomes effective.

ii. If Customer does not object or terminate within the notice period, Customer shall be deemed to have accepted the amended DPA.

(d) **Administrative Amendments**: Verifalia may make administrative, clarifying, or non-material amendments to this DPA (such as correcting typographical errors, updating contact information, or renumbering provisions) without prior notice, provided such amendments do not materially reduce Customer's rights or increase Customer's obligations under this DPA.

(e) **Legally Mandated Amendments**: If an amendment is required by Applicable Data Protection Laws, a Supervisory Authority order, or a court decision, such amendment shall take effect immediately upon notice to Customer, notwithstanding the notice periods in subsection (b).

16.3 Confidentiality

(a) Each Party agrees to maintain the confidentiality of the other Party's Confidential Information disclosed in connection with this DPA, using the same degree of care it uses to protect its own confidential information of a similar nature, but in no event less than reasonable care.

(b) "**Confidential Information**" means this DPA, the Standard Contractual Clauses, information regarding security measures, audit reports, Personal Data Breach details, and any other non-public information disclosed by one Party to the other that is marked as confidential or that a reasonable person would understand to be confidential given the nature of the information and circumstances of disclosure.

(c) Confidential Information does not include information that:

i. Was publicly available at the time of disclosure or subsequently becomes publicly available through no breach of this DPA;

ii. Was rightfully known to the receiving Party prior to disclosure without confidentiality obligations;

iii. Is independently developed by the receiving Party without reference to the disclosing Party's Confidential Information;

iv. Is rightfully obtained from a third party without breach of confidentiality obligations.

(d) A Party may disclose Confidential Information:

i. To its employees, officers, directors, contractors, and professional advisors who have a legitimate need to know and who are bound by confidentiality obligations at least as protective as those in this DPA;

ii. To Subprocessors, to the extent necessary to fulfill obligations under this DPA, provided such Subprocessors are bound by equivalent confidentiality obligations;

iii. As required by Applicable Data Protection Laws, court order, or regulatory authority, provided the disclosing Party (to the extent legally permitted) provides advance notice to the other Party and reasonably cooperates to limit the scope of disclosure.

16.4 Entire Agreement (Data Protection)

This DPA, together with the Agreement and the documents expressly incorporated by reference (including the Standard Contractual Clauses in Annex 4, the Privacy Policy, and the Cookie Policy), constitutes the entire agreement between the Parties with respect to the Processing of Customer Data and supersedes all prior or contemporaneous agreements, understandings, representations, and communications (whether written or oral) relating to such subject matter.

16.5 Severability

If any provision of this DPA is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction or Supervisory Authority, such provision shall be modified and interpreted to accomplish the objectives of such provision to the greatest extent possible under Applicable Data Protection Laws, and the remaining provisions shall continue in full force and effect.

16.6 Waiver

No failure or delay by either Party in exercising any right, power, or remedy under this DPA shall constitute a waiver of such right, power, or remedy. No waiver of any provision of this DPA shall be effective unless in writing and signed by the Party against whom the waiver is sought to be enforced.

16.7 Governing Law and Dispute Resolution

(a) Governing Law:

i. The interpretation, validity, and performance of this DPA shall be governed by the laws of **Italy**, without regard to its conflict of law principles.

ii. Notwithstanding subsection (i), the substantive data protection obligations under this DPA shall be interpreted in accordance with the **GDPR** and other Applicable Data Protection Laws, which shall prevail over Italian law to the extent of any conflict with respect to data protection matters.

iii. Where Customer is subject to mandatory consumer protection, data protection, or other laws in Customer's jurisdiction that cannot be waived or superseded by Italian law, such mandatory laws shall apply to the extent required.

(b) **Dispute Resolution**:

i. **Negotiation**: The Parties agree to attempt to resolve any dispute arising out of or related to this DPA through good-faith negotiations before pursuing formal dispute resolution. Either Party may initiate negotiations by providing written notice to the other Party describing the dispute.

ii. **Arbitration**: If the Parties are unable to resolve a dispute through negotiation within thirty (30) calendar days of the initial notice, the dispute shall be resolved exclusively by binding arbitration in accordance with the rules of the **Camera Arbitrale di Padova** (Arbitration Chamber of the Padua Chamber of Commerce).

- The arbitration shall be conducted in **Padova, Italy**.
- The language of the proceedings shall be **Italian**, unless the Parties agree otherwise in writing.
- The arbitrator's decision shall be final and binding on both Parties and may be enforced in any court of competent jurisdiction.

iii. **Exceptions to Arbitration**: Notwithstanding subsection (ii), either Party may seek injunctive or other equitable relief in a court of competent jurisdiction to prevent infringement of intellectual property rights, unauthorized access to the Services or Personal Data, or breach of confidentiality obligations, without first pursuing arbitration.

iv. **Supervisory Authority Jurisdiction**: Nothing in this Article 16.7 limits the jurisdiction or authority of any Supervisory Authority to investigate, enforce, or adjudicate matters relating to Applicable Data Protection Laws. Data Subjects retain all rights to lodge complaints with Supervisory Authorities or seek judicial remedies in accordance with Applicable Data Protection Laws, notwithstanding the arbitration provisions in this DPA.

(c) **Consumer Rights**:

If Customer is a consumer within the meaning of applicable consumer protection laws (including EU Directive 2011/83/EU), Customer may have additional rights regarding dispute resolution and jurisdiction, including the right to bring proceedings in Customer's country of residence. Nothing in this DPA affects such statutory rights.

(d) **Online Dispute Resolution (EU Consumers)**:

If Customer is a consumer resident in the European Union and is dissatisfied with the resolution of a complaint, Customer may access the European Commission's Online Dispute Resolution platform at https://ec.europa.eu/consumers/odr.

16.8 Notices

(a) All notices, requests, consents, and other communications required or permitted under this DPA must be in writing and shall be deemed given:

i. When delivered personally;

ii. When sent by confirmed email (with read receipt or confirmation of delivery);

iii. Three (3) business days after being sent by registered or certified mail, return receipt requested; or

iv. One (1) business day after deposit with an internationally recognized overnight courier.

(b) **Notices to Verifalia** shall be sent to:

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

Email: support@verifalia.com

(c) **Notices to Customer** shall be sent via email to the preferred contact methods associated with Customer's account administrators as registered in the Services.

(d) Either Party may update its notice contact information by providing written notice to the other Party in accordance with this Article 16.8.

16.9 Assignment

(a) Customer may not assign, transfer, delegate, or sublicense any of its rights or obligations under this DPA without Verifalia's prior written consent.

(b) Verifalia may assign or transfer its rights and obligations under this DPA, in whole or in part, to any affiliate, subsidiary, or successor in interest, including in connection with a merger, acquisition, reorganization, or sale of assets, without Customer's consent, provided that the assignee agrees to be bound by the terms of this DPA.

(c) Any attempted assignment in violation of this Article 16.9 shall be null and void.

(d) Subject to the foregoing, this DPA shall bind and inure to the benefit of the Parties and their respective permitted successors and assigns.

16.10 Third-Party Beneficiaries

(a) Except as expressly provided in subsection (b), this DPA does not and is not intended to confer any rights or remedies upon any person or entity other than the Parties.

(b) **Data Subject Rights**: Data Subjects are intended third-party beneficiaries of this DPA with respect to provisions that directly concern their rights under Applicable Data Protection Laws, including:

- Article 4.2 (Prohibited Data)
- Article 5.1 (Confidentiality)
- Article 7 (Data Security)
- Article 8 (Personal Data Breaches)
- Article 9 (Data Subject Rights)
- Article 11 (Deletion and Return of Personal Data)
- Article 13 (International Data Transfers)
- Article 14.1.2 (Data Subject Compensation Claims)
- Annex 4 (Standard Contractual Clauses)

Data Subjects may enforce these provisions directly against the Parties to the extent permitted by Applicable Data Protection Laws.

16.11 Language

This DPA 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**.

16.12 Counterparts and Electronic Signatures

(a) This DPA may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument.

(b) Customer agrees to the use of electronic records and electronic signatures in connection with this DPA and consents to receive this DPA and any amendments electronically (including via email or posting on the Services).

(c) Customer agrees that electronic signatures (including click-through acceptance, typed names, or digitally signed documents) have the same legal effect as handwritten

signatures and waives any rights or requirements under any law requiring an original (non-electronic) signature or delivery or retention of non-electronic records.

(d) **Specific Approval of Key Clauses (Italian Law)**: In accordance with Article 1341 of the Italian Civil Code, Customer specifically approves the following clauses by accepting this DPA:

- Article 9.4 (costs for complex Data Subject request assistance)
- Article 10.4 (costs for DPIA assistance)
- Article 12.3(c) and 12.4(f) (costs for audits)
- Article 13.2(b) (Customer as data importer for restricted transfers)
- Article 14.2 (limitations of liability)
- Article 14.3 (Customer indemnification obligations)
- Article 16.4 (arbitration)

Article 16.13: Data Protection Contact

Verifalia's **Data Protection Officer** appointed in accordance with GDPR Article 37 is:

Efran Cobisi, Chief Technology Officer
Cobisi Research
Via Della Costituzione, 31
35010 Vigonza (PD), Italy
Email: dpo@verifalia.com

Customer may contact this address for questions or concerns regarding data processing, security, or compliance with this DPA.

ANNEX 1: DETAILS OF PROCESSING

This Annex 1 describes the details of the Processing of Customer Data by Verifalia on behalf of Customer, as required by GDPR Article 28(3) and the Standard Contractual Clauses.

A. LIST OF PARTIES

Data Exporter (Controller):

- **Name**: As specified in the Agreement (Customer)
- **Address**: As specified in Customer's account registration
- **Contact person's name, position, and contact details**: The individual(s) designated by Customer with authority to manage the account and issue Processing instructions
- **Activities relevant to the data transferred**: Use of Verifalia's email verification services to validate and assess the quality of email addresses for Customer's business purposes (such as maintaining email list hygiene, reducing bounce rates, improving email deliverability, preventing fraud, or verifying user registrations)
- **Role**:
  - **Controller**, where the Customer submits personal data (such as email addresses) for verification on its own behalf or for its own business purposes.
  - **Processor**, where the Customer acts on behalf of a third-party Controller (e.g., when reselling or integrating the Verifalia service within its own offerings to end clients).

  In the latter case, the Customer is responsible for ensuring that its own Controller clients have authorized the engagement of Verifalia as a Sub-Processor and that appropriate data transfer and processing arrangements are in place throughout the processing chain.

Data Importer (Processor):

- **Name**: Cobisi Research (operating under the trade name Verifalia)
- **Address**: Via Della Costituzione, 31, 35010 Vigonza (PD), Italy, European Union
- **Contact person's name, position, and contact details**:
  - Verifalia Support Team
    Email: support@verifalia.com

- **Activities relevant to the data transferred**: Provision of cloud-based email verification services, including technical validation, syntax checking, domain verification, mailbox existence verification, SMTP transaction simulation, deliverability assessment, and quality scoring
- **Role**:
  - **Processor**, where processing personal data on behalf of the Customer acting as Controller.
  - **Sub-Processor**, where processing personal data on behalf of the Customer acting as Processor (in the reseller or proxy-integration model).

B. DESCRIPTION OF TRANSFER(S)

Categories of Data Subjects whose personal data is transferred:

- Individuals whose email addresses are submitted by Customer to the Services for verification
- Typically includes: Customer's subscribers, users, leads, customers, website visitors, or other individuals with whom Customer communicates or intends to communicate via email
- May include prospective or existing customers, newsletter subscribers, event registrants, account holders, or any other natural persons whose email addresses Customer seeks to verify

Categories of Personal Data transferred:

- **Primary Data**: Email addresses
- **Incidental Personal Data**: Verification job name, custom reference strings (if containing Personal Data, contrary to recommendations)
- **Metadata**:
  - Verification result (deliverability classification, DNS records information, SMTP transaction details, timestamps, etc.)
  - IP address of Customer's system submitting the verification request (for security, fraud prevention, and usage analytics purposes)

Note: The email addresses themselves and the collected IP address constitute Personal Data. Verifalia does not intentionally collect or Process any other categories of Personal Data (such as names, postal addresses, telephone numbers, financial information), and Customer is

prohibited from submitting such data under Article 4.2 if it constitutes Special Categories of Personal Data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards:

- **Prohibited**: Customer is expressly prohibited from submitting Special Categories of Personal Data (GDPR Article 9), Personal Data relating to criminal convictions and offences (GDPR Article 10), or Personal Data of children (Article 4.2 of the DPA).
- Verifalia's Services are not designed for or intended to Process sensitive data.
- If Customer breaches this prohibition, Verifalia may immediately suspend Processing and require deletion, and Customer shall indemnify Verifalia for any resulting liability.

The frequency of the transfer:

- Continuous and ongoing throughout the term of the Agreement, as determined by Customer
- Customer may submit email addresses for verification at any time and frequency, subject to usage limits and rate limits specified in Customer's Subscription Plan

Nature of the Processing:

- Automated technical verification and validation of email addresses using AI-powered algorithms, syntax validation, DNS queries, SMTP transactions, and domain/mailbox checks
- Generation of Verification Results (deliverability assessments, validation status)
- Temporary storage of email addresses and Verification Results in volatile (RAM-only) memory for the retention period configured by Customer (5 minutes to 30 days)
- Automatic deletion of Customer Data upon expiry of the retention period or upon Customer's manual deletion request

Purpose(s) of the data transfer and further Processing:

- To provide the email verification Services to Customer as described in the Agreement
- To enable Customer to:
    - Validate email address syntax and format
    - Verify domain existence and configuration
    - Check mailbox existence and deliverability
    - Assess email address quality and risk

- Maintain email list hygiene
- Reduce email bounce rates
- Improve email deliverability
- Prevent fraud, abuse, or invalid registrations
- Comply with anti-spam laws and email marketing best practices

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

- **Duration of Processing**: Verifalia processes Customer Data in accordance with the tiered retention framework set forth in Article 11.1:

  (a) **Primary Customer Data** (email addresses, verification results, custom reference strings): Stored in volatile (RAM-only) memory for the retention period configured by Customer (5 minutes to 30 days), then automatically and permanently deleted.

  (b) **Incidental Personal Data** (job names, IP addresses): Automatically removed or anonymized when email addresses are deleted (step (a) above).

  (c) **Anonymized Job Records**: Retained for up to 2 years from the date of job creation for legitimate business purposes (billing verification, fraud prevention, service improvement, analytics), then permanently deleted.

Processing duration is determined solely by Customer through configuration of retention periods for verification jobs. Verifalia does not extend retention periods beyond Customer's configuration except as described in Article 11.1(c) for anonymized, non-personal metadata.

- **Automatic Deletion**: Customer Data is automatically and permanently deleted upon expiry of the configured retention period. Deleted data is immediately and irreversibly destroyed and cannot be recovered.
- **Manual Deletion**: Customer may manually delete Customer Data at any time prior to the expiry of the retention period using the deletion functionality in the Services.
- **Upon Termination**: All Customer Data is deleted within 30 days following termination of the Agreement, unless earlier deleted by Customer or automatically deleted upon expiry of retention periods.
- **Legal Retention**: Verifalia does not retain Customer Data beyond the above periods, except to the extent required by applicable law (such as tax, accounting, or anti-money laundering laws), in which case data is isolated and deleted at the earliest time permitted by law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the Processing:

- **Subject Matter**: Provision of cloud infrastructure, computing resources, and data storage to support Verifalia's email verification Services
- **Nature of Processing**: Hosting, storage, and computing infrastructure services; Subprocessors provide raw infrastructure only and do not access, view, or independently Process Customer Data
- **Duration**: For the duration of Verifalia's agreement with each Subprocessor, and in any event no longer than the retention periods specified above
- **Subprocessors**: See Annex 3

C. COMPETENT SUPERVISORY AUTHORITY

For EU Data Exporters:

The competent Supervisory Authority is the Supervisory Authority of the EU Member State in which the Data Exporter (Customer) is established.

If the Data Exporter is not established in the EU, the competent Supervisory Authority is the Supervisory Authority of the EU Member State in which the Data Exporter's EU representative (if any) is located, or the Supervisory Authority with which the Data Exporter has chosen to cooperate.

For UK Data Exporters:

The competent Supervisory Authority is the **UK Information Commissioner's Office (ICO)**.

For Swiss Data Exporters:

The competent Supervisory Authority is the **Swiss Federal Data Protection and Information Commissioner (FDPIC)**.

For the Data Importer (Verifalia):

The competent Supervisory Authority is the **Italian Data Protection Authority (Garante per la protezione dei dati personali)**, as Verifalia is established in Italy.

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

This Annex 2 describes the technical and organisational measures implemented by Verifalia to ensure the security of Customer Data, in accordance with GDPR Article 32 and Article 7 of this DPA.

Verifalia has implemented and maintains the following categories of security measures. These measures are subject to technical progress and development, and Verifalia may update or modify them from time to time to ensure ongoing compliance with Applicable Data Protection Laws and to address evolving security threats.

1. MEASURES OF ENCRYPTION AND SEGREGATION OF PERSONAL DATA

Encryption in Transit:

- All data transmitted between Customer and Verifalia's Services is encrypted using **Transport Layer Security (TLS)**.
- Older, insecure protocols (such as SSL) are disabled.
- Strong cipher suites are enforced, and weak or deprecated ciphers are rejected.

Encryption at Rest:

- Customer Data stored in volatile (RAM-only) memory is encrypted using **AES-256** encryption (or similar) where technically feasible.
- Disk-based storage (if any, such as for temporary file uploads) is encrypted using industry-standard encryption.

Cryptographic Key Management:

- Encryption keys are managed using industry-standard key management practices.
- Access to encryption keys is restricted to authorized personnel and systems on a need-to-know basis.
- Keys are rotated periodically in accordance with security best practices.

Logical Segregation:

- Customer Data is isolated per Customer account using logical access controls, ensuring that one Customer's data cannot be accessed by another Customer or unauthorized parties.

2. MEASURES FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY, AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

2.1 Confidentiality

Access Controls:

- **Role-Based Access Control (RBAC):** Access to Customer Data and Verifalia's systems is restricted based on job role and function. Users are granted the minimum level of access necessary to perform their duties (principle of least privilege).
- **Fine-Grained User Permissions:** Customer may configure granular user permissions within the Services to control which users can access, modify, or delete Customer Data.
- **Multi-Factor Authentication (MFA):** Customer may require users to use multi-factor authentication while accessing the Services.
- **Client Certificate Authentication (X.509 TLS):** Certain Subscription Plans support client certificate authentication for API access, providing an additional layer of authentication security.

Authentication and Password Security:

- User passwords are hashed using **industry-standard cryptographic hashing algorithms (bcrypt**, or equivalent**)** with unique salts.
- Passwords are never stored in plaintext.
- Password policies enforce minimum complexity requirements.

Personnel Confidentiality:

- All Verifalia personnel with access to Customer Data are subject to binding confidentiality obligations (contractual or statutory).
- Personnel receive training on data protection, confidentiality, and security obligations.

Subprocessor Confidentiality:

- All Subprocessors are contractually required to implement equivalent confidentiality measures and to ensure their personnel are bound by confidentiality obligations.

2.2 Integrity

Data Integrity Controls:

- Customer Data is processed in accordance with Customer's instructions and is not modified, altered, or used for any purpose other than providing the Services.
- Checksums and integrity verification mechanisms are used to detect corruption or unauthorized modification of data during transmission and storage.

Change Management:

- Changes to Verifalia's systems, infrastructure, and software are subject to documented change management processes, including testing, approval, and rollback procedures.

2.3 Availability

Redundancy and Fault Tolerance:

- Verifalia's Services are hosted on redundant infrastructure provided by Subprocessors (Hetzner, AWS, myLoc, M247) across multiple data centers within Germany (EU).
- Load balancing and failover mechanisms are implemented to ensure service continuity in the event of hardware or network failures.

Data Center Reliability:

Subprocessor data centers feature:

- Redundant power supplies and backup generators
- Redundant network connectivity
- Climate control and fire suppression systems
- 24/7 monitoring and on-site security personnel

Uptime Commitments:

Certain Subscription Plans include uptime guarantees as specified in Verifalia's Service Level Agreement (SLA), available at https://verifalia.com/legal/service-level-agreement

Monitoring and Incident Response:

- Verifalia implements continuous monitoring of Services availability, performance, and security.
- Automated alerting mechanisms notify Verifalia personnel of outages, performance degradation, or security incidents.
- Incident response procedures are in place to rapidly investigate, contain, and remediate incidents.

2.4 Resilience

Disaster Recovery:

- Verifalia has implemented disaster recovery procedures to restore Services in the event of a catastrophic failure.
- Given the volatile (RAM-only) nature of Customer Data storage, disaster recovery focuses on restoring service availability rather than data recovery (as Customer Data is automatically deleted upon expiry of retention periods and cannot be recovered post-deletion).

Business Continuity:

Verifalia maintains business continuity plans to ensure continuity of critical operations during disruptive events (natural disasters, cyberattacks, pandemics).

3. MEASURES FOR ENSURING THE ABILITY TO RESTORE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT

Backup and Recovery (Infrastructure):

Verifalia's infrastructure (application code, configuration, databases for account management and billing - **not Customer Data**) is backed up regularly.

Backups are stored securely and are tested periodically to ensure recoverability.

Customer Data Recovery:

Important: Customer Data (email addresses and Verification Results) is stored in volatile (RAM-only) memory and is not backed up.

- Once Customer Data is deleted (automatically upon expiry of the retention period, manually by Customer, or upon termination), it is **immediately and permanently destroyed** and **cannot be recovered or restored**.
- Customer is responsible for downloading and retaining Verification Results as soon as they are available and prior to expiry of the retention period if Customer requires long-term retention.

Incident Recovery:

- In the event of a technical incident affecting Service availability, Verifalia will prioritize restoring Services in accordance with the SLA (if applicable).
- Customers will be notified of significant incidents affecting availability in accordance with the SLA and Article 8 of this DPA (for Personal Data Breaches).

4. PROCESSES FOR REGULARLY TESTING, ASSESSING, AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES

Security Assessments and Testing:

- **Vulnerability Assessments**: Verifalia conducts periodic vulnerability scans and assessments of its infrastructure, applications, and Services to identify and remediate security weaknesses.
- **Penetration Testing**: Verifalia engages qualified third-party security professionals to conduct penetration tests of its Services on a periodic basis.
- **Security Monitoring**: Verifalia implements intrusion detection and prevention systems (IDS/IPS) to monitor for suspicious activity, unauthorized access attempts, and security threats.

Compliance Reviews:

- Verifalia regularly reviews and updates its security policies, procedures, and measures to ensure ongoing compliance with Applicable Data Protection Laws and industry best practices.
- Internal audits and compliance assessments are conducted periodically.

Subprocessor Assurance:

- Verifalia reviews Subprocessors' security measures, certifications, and audit reports (where available) to ensure they meet or exceed Verifalia's security standards.
- Subprocessor agreements require Subprocessors to maintain appropriate security measures and to notify Verifalia of any security incidents.

Continuous Improvement:

Security measures are updated and improved in response to:

- Findings from security assessments and audits
- Emerging security threats and vulnerabilities
- Changes in Applicable Data Protection Laws or regulatory guidance
- Technological advancements and industry best practices

5. MEASURES FOR USER IDENTIFICATION AND AUTHORISATION

User Authentication:

- All Users (including Customer's personnel and Verifalia's personnel) must authenticate using unique credentials (username and password, or client certificates) before accessing the Services or Customer Data.
- Multi-factor authentication (MFA) is available to Customers and is required for Verifalia personnel with access to production systems.

Authorisation and Access Control:

Access to Customer Data is restricted to:

- Customer's authorized Users, as configured by Customer through the Services' user management functionality
- Verifalia personnel on a strict need-to-know basis (e.g., for customer support, security incident investigation, or legal compliance), subject to confidentiality obligations
- Subprocessors, solely to the extent necessary to provide infrastructure services (and without visibility into unencrypted Customer Data)

API Security:

- API access is authenticated using username/password authentication, or client certificate authentication (X.509 TLS).
- API rate limiting is enforced to prevent abuse and denial-of-service attacks.

6. MEASURES FOR THE PROTECTION OF DATA DURING TRANSMISSION

Encryption in Transit:

- As described in Section 1 above, all data transmitted between Customer and Verifalia is encrypted using TLS.
- Encryption is enforced for all connections; unencrypted (plaintext) connections and connections using older SSL protocols are rejected.

Network Security:

- Verifalia's network infrastructure is protected by firewalls, intrusion detection/prevention systems, and network segmentation.
- Unnecessary network services and ports are disabled.
- Network traffic is monitored for suspicious activity.

Data Transmission to Subprocessors:

- Data transmitted to Subprocessors (for infrastructure services) is encrypted in transit and at rest.
- Subprocessors are located exclusively within the EU (Germany) and do not have visibility into unencrypted Customer Data.

7. MEASURES FOR THE PROTECTION OF DATA DURING STORAGE

Volatile Storage:

Customer Data is stored exclusively in **volatile (RAM-only) memory**, which is:

- Non-persistent (data is lost on power loss or server restart)
- Automatically cleared upon expiry of the configured retention period
- Not written to disk (except temporarily for file uploads, which are immediately deleted after processing)

This approach minimizes the risk of unauthorized access, data breaches, or long-term data exposure.

Encryption at Rest:

As described in Section 1 above, Customer Data is encrypted at rest using AES-256 or equivalent encryption.

Physical Security (Subprocessor Data Centers):

Verifalia relies on Subprocessors' data centers for physical security. These data centers implement:

- Video-monitored high-security perimeter fencing
- Electronic access control terminals with transponder keys or admission cards
- 24/7 surveillance cameras monitoring access routes, entrances, and server rooms
- Biometric access controls and security door interlocking systems
- On-site security personnel
- Environmental controls (fire suppression, climate control, flood protection)

Logical Isolation:

- Customer Data is logically isolated per Customer account, ensuring that one Customer's data cannot be accessed by another Customer.
- Verifalia's multi-tenant architecture implements strict access controls and data segregation mechanisms.

8. MEASURES FOR ENSURING PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED

Verifalia does not own or operate physical data centers. Physical security is provided by Subprocessors' data centers, which implement the measures described in Section 7 above.

Verifalia's registered office (Via Della Costituzione 31, 35010 Vigonza, Italy) implements standard physical security measures appropriate for an administrative office environment, including locked premises, access control, and alarm systems. Customer Data is not stored or processed at Verifalia's office locations.

9. MEASURES FOR ENSURING EVENTS LOGGING

Audit Logs and Event Logging:

Verifalia maintains comprehensive audit logs of events related to Customer Data and Services usage, including:

- User authentication and access events
- API requests and responses (excluding the content of Customer Data, for privacy and performance reasons)
- Data access, modification, and deletion events
- Administrative actions (account changes, user management, configuration changes)
- Security events (failed login attempts, intrusion detection alerts, anomalous activity)

Log Retention:

Logs are retained for a period consistent with security, operational, and legal requirements.

Logs related to Personal Data Breaches or security incidents are retained for longer periods as required by Applicable Data Protection Laws.

Log Protection:

Audit logs are protected from unauthorized access, modification, or deletion.

Access to logs is restricted to authorized Verifalia personnel (such as security, compliance, and operations teams).

Log Monitoring and Analysis:

Logs are monitored and analyzed (manually and via automated tools) to detect security incidents, anomalous activity, or policy violations.

Automated alerting mechanisms notify Verifalia personnel of suspicious events.

10. MEASURES FOR ENSURING SYSTEM CONFIGURATION

Secure Configuration Management:

Verifalia's systems and infrastructure are configured in accordance with security best practices and industry standards (such as OWASP guidelines).

Unnecessary services, applications, and network ports are disabled.

Security patches and updates are applied promptly in accordance with Verifalia's patch management policy.

Configuration Baselines:

Verifalia maintains documented configuration baselines for its systems and infrastructure.

Configuration changes are subject to change management processes (testing, approval, documentation, rollback procedures).

Hardening:

Operating systems, databases, and applications are hardened to reduce attack surface and mitigate security risks.

Default passwords and credentials are changed immediately upon deployment.

11. MEASURES FOR ENSURING DATA MINIMISATION

Processing Limited to Necessary Data:

Verifalia Processes only the Personal Data necessary to provide the Services: email addresses and associated verification metadata.

Verifalia does not collect or Process any other categories of Personal Data unless strictly necessary for providing the Services or complying with legal obligations.

Temporary Storage:

Customer Data is stored only for the retention period configured by Customer (5 minutes to 30 days). Data is automatically and permanently deleted upon expiry of the retention period: Verifalia does not retain Customer Data longer than necessary.

No Secondary Use:

Verifalia does not use Customer Data for any purpose other than providing the Services to Customer.

Verifalia does not sell, rent, lease, or disclose Customer Data to third parties for marketing or other purposes.

12. MEASURES FOR ENSURING DATA QUALITY

Data Accuracy:

Verifalia Processes Customer Data as submitted by Customer and does not modify email addresses (except for normalization, such as trimming whitespace or converting to lowercase, where necessary for technical processing).

Customer is solely responsible for the accuracy and quality of Customer Data submitted to the Services.

Verification Accuracy:

Verifalia uses AI-powered algorithms, industry-standard validation techniques, and continuous improvement processes to ensure the accuracy and reliability of Verification Results.

However, as disclosed in Section 12.2 of the Agreement and Article 5.6 of this DPA, Verification Results may not always be 100% accurate due to the probabilistic nature of AI and external factors beyond Verifalia's control (such as temporary mail server outages, greylisting, or anti-spam measures).

13. MEASURES FOR ENSURING LIMITED DATA RETENTION

Configurable Retention Periods:

Customer may configure data retention periods between 5 minutes and 30 days for each email verification job.

Customer Data is automatically deleted upon expiry of the configured retention period.

Immediate and Permanent Deletion:

Deleted Customer Data is immediately and irreversibly destroyed and cannot be recovered.

Verifalia does not maintain backups or archives of deleted Customer Data.

Deletion Upon Termination:

All Customer Data is deleted within 30 days following termination of the Agreement (or earlier, if retention periods expire sooner).

14. MEASURES FOR ENSURING ACCOUNTABILITY

Data Protection Policies:

Verifalia has implemented and maintains comprehensive data protection policies and procedures, including:

- Data processing and security policies
- Incident response and breach notification procedures
- Subprocessor management and vetting procedures
- Employee training and awareness programs

Compliance Monitoring:

Verifalia monitors compliance with this DPA and Applicable Data Protection Laws through regular audits, assessments, and reviews.

Documentation:

Verifalia maintains records of Processing activities, security measures, Subprocessor agreements, and compliance activities as required by GDPR Article 30 and this DPA.

Cooperation with Supervisory Authorities:

Verifalia cooperates with Supervisory Authorities and responds to inquiries, audits, and enforcement actions in accordance with Applicable Data Protection Laws.

15. MEASURES FOR ALLOWING DATA PORTABILITY AND ENSURING ERASURE

Data Portability:

- Customer may access and export Verification Results at any time via the Services in commonly used, machine-readable formats (JSON, CSV, Excel).

- APIs and user interfaces provide self-service data export functionality.

Data Erasure:

- Customer may manually delete Customer Data at any time via the Services' deletion functionality.
- Deleted data is immediately and permanently destroyed and cannot be recovered.
- Automatic deletion occurs upon expiry of the configured retention period.

Note: The technical and organisational measures described in this Annex 2 are subject to technical progress and development. Verifalia may update or modify these measures from time to time to ensure ongoing compliance with Applicable Data Protection Laws, address evolving security threats, and incorporate technological advancements. Material changes to security measures will be communicated to Customer in accordance with Article 7.3 of this DPA.

ANNEX 3: LIST OF SUBPROCESSORS

This Annex 3 lists the Subprocessors currently authorized by Customer to Process Customer Data on behalf of Verifalia, in accordance with Article 6 of this DPA.

Verifalia engages the following Subprocessors exclusively to provide infrastructure, computing, and storage services to support the email verification Services. These Subprocessors provide raw infrastructure only and do not access, view, or independently Process Customer Data (email addresses or Verification Results) in unencrypted form.

All Subprocessor data centers are located within the European Economic Area (EEA), specifically in Germany.

Subprocessor Name	Service Provided	Location of Processing	Data Center Locations
Hetzner Online GmbH	Computing infrastructure, storage	Germany (EU)	Nuremberg, Germany; Falkenstein, Germany
Amazon Web Services, Inc. (AWS)	Computing infrastructure, storage	Germany (EU)	Frankfurt, Germany (Region: eu-central-1)
myLoc managed IT AG	Computing infrastructure	Germany (EU)	Düsseldorf, Germany
M247 Europe S.R.L.	Computing infrastructure	Germany (EU)	Frankfurt, Germany

ADDITIONAL INFORMATION

Nature of Processing by Subprocessors:

- **Hosting and Infrastructure**: Provision of physical and virtual servers, computing resources, network infrastructure, and data center facilities.
- **Storage**: Provision of volatile (RAM) and temporary storage for Customer Data processed by Verifalia's Services.
- **Security**: Implementation of physical security, environmental controls, network security, and infrastructure-level security measures.

No Direct Access to Customer Data:

- Subprocessors provide infrastructure services only and do not have visibility into or access to unencrypted Customer Data.
- Customer Data is encrypted in transit (TLS) and at rest (AES-256).
- Subprocessors do not perform any operations on Customer Data (such as analysis, profiling, or verification); such operations are performed exclusively by Verifalia's software running on Subprocessor infrastructure.

Subprocessor Obligations:

Verifalia has entered into written agreements with each Subprocessor that impose data protection obligations equivalent to those set forth in this DPA, including obligations regarding security, confidentiality, data subject rights, breach notification, and international transfers.

Verifalia remains fully liable to Customer for the performance of each Subprocessor's obligations.

Changes to Subprocessors:

Verifalia may add, remove, or replace Subprocessors from time to time in accordance with Article 6.3 of this DPA (notification and objection mechanism).

The current version of this Annex 3 is available to Customer via the Services or upon written request to support@verifalia.com.

ANNEX 4: STANDARD CONTRACTUAL CLAUSES

This Annex 4 applies solely to the extent that Verifalia, acting as a data processor established in the European Economic Area, transfers or otherwise makes personal data available to the **Customer located in a country outside the EEA** that does not benefit from an adequacy decision pursuant to Article 45 GDPR (a "Restricted Transfer").

A. EU STANDARD CONTRACTUAL CLAUSES (GDPR)

For transfers of Personal Data subject to the **GDPR** that involve or are reasonably likely to involve a Restricted Transfer (including when Customer, located outside the EEA, accesses or downloads Customer Data from the Services), the Parties agree to comply with the **Standard Contractual Clauses for the transfer of personal data to third countries** adopted by **European Commission Implementing Decision 2021/914 of 4 June 2021**, available at:

https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

The SCCs are incorporated into this DPA as if set forth in full and form an integral part of this DPA.

Specifications for EU SCCs:

Module:

- **Module Four (Processor to Controller)** applies where:
    - **Customer** = data importer (Controller established in or accessing data from a third country)
    - **Verifalia** = data exporter (Processor established in EU)

    This module governs the transfer of Verification Results from Verifalia (acting as Processor) to Customer (acting as Controller or as intermediary on behalf of end Controllers), when Customer accesses or downloads such data from the Services.

Note on Reseller/Agency Customers: Where Customer acts as a Processor or intermediary on behalf of Customer's own clients (end Controllers), Customer receives Verification Results under Module Four and is responsible for ensuring that any onward transfer or delivery of such results to Customer's clients complies with Applicable Data Protection Laws and includes appropriate safeguards.

Clause 7 (Docking Clause):

The optional docking clause is available for accession by authorized third parties in accordance with the terms of the SCCs.

Clause 9 (Use of Sub-processors):

Not applicable to Module Four.

Verifalia's engagement of Subprocessors is governed by Article 6 of this DPA. Customer's engagement of processors (where Customer acts as Controller) or sub-processors (where Customer acts as Processor for Customer's clients) is governed by Customer's own agreements and obligations under Applicable Data Protection Laws.

Clause 11 (Redress):

Option 1 applies: Any dispute between a data subject and one of the Parties arising out of the SCCs shall be resolved in accordance with Clause 18 (Choice of forum and jurisdiction).

Clause 17 (Governing Law):

The SCCs shall be governed by the law of **Italy**, being the EU Member State in which the data exporter (Verifalia) is established, in accordance with Clause 17(a) of the SCCs.

Clause 18 (Choice of Forum and Jurisdiction):

The courts of **Italy** shall have jurisdiction over disputes arising out of the SCCs.

Data subjects may also bring proceedings before the courts of the EU Member State in which they have habitual residence, in accordance with Clause 18(c) of the SCCs.

Annexes to the EU SCCs:

- **Annex I (Information about the Parties, Transfer, and Processing):**
  - **Part A (List of Parties):**
    - Data exporter: Verifalia (contact details as set forth in Annex 1, Section A of this DPA)
    - Data importer: Customer (contact details as set forth in Annex 1, Section A of this DPA)
  - **Part B (Description of Transfer)**: The transfer occurs when Customer accesses or downloads Verification Results (Customer Data) from the Services. The categories of data subjects, categories of personal data, sensitive data restrictions, frequency, nature, purpose, and retention period are as set forth in Annex 1, Section B of this DPA.

    - **Part C (Competent Supervisory Authority)**: The Italian Data Protection Authority (Garante per la protezione dei dati personali), as Verifalia (data exporter) is established in Italy.

- **Annex II (Technical and Organisational Measures):**
    - Completed by reference to **Annex 2 (Technical and Organizational Measures)** of this DPA, describing the measures implemented by Verifalia (data exporter).
- **Annex III (List of Sub-processors):**
    - Not applicable to Module Four. Verifalia's Subprocessors are listed in **Annex 3** of this DPA and governed by Article 6.

B. UK INTERNATIONAL DATA TRANSFER ADDENDUM (UK GDPR)

For transfers of Personal Data subject to the **UK GDPR** that involve or are reasonably likely to involve a Restricted Transfer (including when Customer, located outside the UK, accesses or downloads Customer Data from the Services), the Parties agree to comply with the **International Data Transfer Addendum to the EU Commission Standard Contractual Clauses** (version **B1.0**, in force 21 March 2022), issued by the **UK Information Commissioner's Office (ICO)**, available at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/

The UK IDTA is incorporated into this DPA as if set forth in full and applies in addition to (and as an addendum to) the EU Standard Contractual Clauses set forth in Section A above.

Specifications for UK IDTA:

Parties:

- **Exporter**: Verifalia (Processor established in EEA)
- **Importer**: Customer (Controller or intermediary established in or accessing data from a third country)

Tables to the UK IDTA:

- **Table 1 (Parties):**
    - Completed by reference to Annex 1, Section A of this DPA, with Verifalia as exporter and Customer as importer.

- **Table 2 (Approved EU SCCs):**
  - The Approved EU SCCs are the **EU Standard Contractual Clauses adopted by European Commission Implementing Decision 2021/914**, as specified in Section A above.
  - **Applicable Module**: Module Four (Processor to Controller).
- **Table 3 (Annexes):**
  - Completed by reference to Annexes 1, 2, and 3 of this DPA (as specified in Section A above).
- **Table 4 (Optional Clauses):**
  - No optional clauses are selected.

Governing Law and Jurisdiction:

Disputes arising out of the UK IDTA shall be governed by the laws of **England and Wales** and subject to the jurisdiction of the courts of **England and Wales**, in accordance with the UK IDTA.

C. ADDITIONAL PROVISIONS

Hierarchy:

In the event of any conflict between the Standard Contractual Clauses (EU SCCs or UK IDTA) and any other provision of this DPA or the Agreement, the Standard Contractual Clauses shall prevail with respect to the subject matter governed by the SCCs (international data transfers and related safeguards).

Incorporation:

The SCCs are incorporated by reference and need not be separately executed by the Parties. Customer's acceptance of this DPA (including by click-through acceptance, continued use of the Services, or execution of the Agreement) constitutes acceptance of and agreement to the SCCs.

Updates:

If the European Commission, UK ICO, or other relevant authorities issue updated or replacement SCCs, or if Applicable Data Protection Laws require the use of alternative transfer mechanisms, Verifalia may update this Annex 4 accordingly, subject to Article 16.2 (Amendments) of this DPA.

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

VAT ID: IT04391160282

Website: https://verifalia.com
Email: support@verifalia.com