DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement ("**DPA**"), including its three Exhibits, is an integral part of the Master Subscription Agreement ("**MSA**") between Cleeng and Customer (collectively, the "Parties"). It reflects the Parties' agreement for the Processing of Customer Personal Data and is incorporated into the MSA by reference. By executing the MSA, the Parties agree to this DPA, including the Standard Contractual Clauses in **Exhibit 2**.

All capitalized terms used herein, but not otherwise defined, shall have the meaning defined in the MSA. Except as modified below, the terms of the MSA shall remain in full force and effect.

This DPA does not apply to the Merchant Product, except to the extent Cleeng processes Personal Data for certain operational functionalities (not transaction related) in its capacity as a data processor. For information on our privacy commitments regarding the Merchant Product, including when Cleeng acts as a data controller, please refer to our Privacy Policy.

Although the DPA is incorporated into your MSA and valid without the necessity to put your written signatures in the body of the DPA, your company may require signing a written DPA for evidence or internal compliance purposes. To support our Customers' needs, Cleeng provides a pre-signed version of the DPA. If you intend to execute it for the above reasons, please (i) download a pre-signed copy of the DPA, (ii) countersign it where instructed, and (iii) send back a countersigned copy to privacy@cleeng.com.

1. DEFINITIONS

Key terms are defined as follows:

- **Adequate Country:** A country within the EEA, the UK, Switzerland, or otherwise recognized by the European Commission or Information Commissioner as providing adequate data protection.
- **Authorized Affiliate:** Any of Customer's Affiliates permitted to use the Services under the MSA.
- **CPRA:** The California Privacy Rights Act of 2020, and any regulations promulgated thereunder, as amended or superseded from time to time, which amends the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq.
- **Controller:** The entity determining the purposes and means of Processing Customer Personal Data (including a "business" under CPRA).

- **Customer Personal Data:** The portion of Customer Data (as defined in the MSA) that constitutes personal data/information under Data Protection Laws and Regulations.
- **Data Protection Laws and Regulations:** Includes GDPR, CPRA, UK GDPR, Swiss Federal Act on Data Protection, and other applicable data protection or privacy laws.
- **Data Subject:** Any identified or identifiable natural person or User to whom Customer Personal Data relates.
- **GDPR:** The General Data Protection Regulation (Regulation (EU) 2016/679).
- **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
- **Process / Processing:** Any operation performed on Customer Personal Data.
- **Processor:** The entity Processing Customer Personal Data on behalf of the Controller (including a "service provider" under CPRA).
- **Request:** A Data Subject Access Request, meaning a request by a Data Subject to exercise their rights (e.g., access, rectification, erasure).
- **Restricted Transfer:** A transfer of Customer Personal Data to a country outside the EEA, UK, or Switzerland without an adequacy decision.
- **Security Documentation:** Cleeng's third-party certifications and audit reports, including SOC 2 Type 2 and other applicable security certifications, which demonstrate compliance with this DPA.
- **Services:** The Subscription Services as specified in the MSA and any Order Forms, excluding Merchant Product.
- **Standard Contractual Clauses (SCCs):** Collectively, the EU SCCs, UK SCCs, and Swiss SCCs, as applicable.
- **Subprocessor:** Any Processor engaged by Cleeng to Process Customer Personal Data as listed at www.cleeng.com/sub-processors-list.
- **Swiss Federal Act on Data Protection:** The Swiss Federal Act on Data Protection of June 19, 1992, as amended, including the revised version (nFADP), and its implementing ordinances.

- **UK GDPR:** The UK General Data Protection Regulation (as incorporated into UK law under the European Union (Withdrawal) Act 2018), and the UK Data Protection Act 2018, both as amended.

2. ROLES AND RESPONSIBILITIES

2.1 Customer as Controller

Customer remains the Controller and is responsible for compliance with Controller obligations under Data Protection Laws, including ensuring legal justification for transmission, providing notices, obtaining consents, and verifying the accuracy and legality of the data acquired. Customer warrants that its use of the Services complies with Data Protection Laws and does not violate Data Subject rights, including opt-out rights under CPRA. Customer warrants that Personal Data will not contain sensitive data, health information, biometric information, or payment card information (except for Customer's own payment details for the Services).

2.2 Cleeng as Processor

Cleeng is the Processor and will Process Customer Personal Data only as necessary for the provision of the Services set forth in the MSA. Cleeng will not Process the data for purposes other than those in the MSA or as instructed by Customer, nor disclose it to third parties other than Affiliates or Subprocessors for the aforementioned purposes, or as required by law.

2.3 Processing Instructions

Cleeng shall Process Customer Personal Data in accordance with Customer's documented instructions, as reflected in the MSA and this DPA. The MSA and this DPA constitute Customer's complete instructions. Cleeng is authorized to instruct Subprocessors. Cleeng shall inform the Customer if an instruction infringes applicable EU Data Protection Laws and Regulations.

2.4 Scope of Processing

The subject matter, duration, nature, purpose, data types, and data subject categories are detailed in **Exhibit 1**.

2.5 Authorized Affiliates

The Customer enters into this DPA on behalf of itself and, as applicable and to the extent required under Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Cleeng and each such Authorized Affiliate. Customer warrants that each Authorized Affiliate agrees to be bound by the obligations under this DPA.

3. CATEGORIES OF PERSONAL DATA, DATA SUBJECTS, AND RESTRICTIONS

3.1 Categories of Personal Data

Cleeng is authorized to Process the following categories to perform the Services:

- **Contact & User Data:** Name, address, e-mail, phone number, and associated time zone information or similar.
- **Technical Data:** User IDs, location data, connection data, IP address, device information, login credentials and authentication tokens.
- **Financial Data:** Bank account information, billing address, transaction history, subscription status, and payment method details.
- **Subscriber & Usage Data:** Subscriber demographics, login patterns, subscription tier, engagement metrics, content access, platform usage, feature utilization, and customer journey data.
- **Support Data:** Support tickets, communications, and issue resolution history.

3.2 Categories of Data Subjects

- Users (subscribers/viewers) of Customer's services.
- Customer's employees, administrators, contractors, partners, agents, contact persons, authorised signatories and authorized users of the Services.

3.3 Scope and Restrictions

- **Prohibited Data:** Processing of **Special Categories of Data** (GDPR Art. 9) or **Criminal Convictions Data** (GDPR Art. 10) is strictly prohibited unless expressly agreed in writing.
- **Non-Compliant Data Consequences:** Customer is solely responsible for consequences and shall indemnify Cleeng for any claims arising from providing unauthorized data.

4. CLEENG PERSONNEL

Cleeng shall ensure personnel processing Customer Personal Data are subject to confidentiality obligations, are reliably trained , and have access limited by the principle of least privilege.

Cleeng and its Affiliates have appointed a data protection officer who may be reached at privacy@cleeng.com.

5. SUBPROCESSORS

5.1 General Authorization

Customer grants general written authorization for Cleeng's use of Subprocessors. Cleeng ensures each Subprocessor agrees in writing to act only on Cleeng's instructions and to protect the data to a standard substantially the same as this DPA. Cleeng is liable for the acts and omissions of its Subprocessors.

5.2 Current Subprocessors

A list of current Subprocessors is included at www.cleeng.com/sub-processors-list **(List of Subprocessors)** and is acknowledged by the Customer as of the DPA Effective Date.

5.3 Changes and Objection

Cleeng shall provide at least fourteen (14) days advance notice of any addition or replacement of Subprocessors by posting such changes on a dedicated, easily accessible Subprocessor Page on Cleeng's website. Customers may subscribe to an RSS feed or email notification list for this page to receive active notice. Customer may object within the 14-day notice period with written notice to privacy@cleeng.com. If Cleeng does not receive a Customer objection within the 14-day period, the Customer will be deemed to have consented to the appointment of the new Subprocessor.

Upon receipt of a Customer objection, Cleeng will use reasonable efforts to: (i) Make available to Customer a change in the Service; or (ii) Recommend a commercially reasonable change to the Customer's configuration or use of the Service to avoid Processing Customer Personal Data by the objected-to Subprocessor without materially burdening the Customer.

If Cleeng is unable to make available such change within a reasonable time, the Parties will meet and confer to determine if the Customer objection can be resolved. If the Parties are unable to reach a resolution, the Customer's sole right is to terminate the transfer of Customer Personal Data and the applicable or part of the applicable Order Form(s) with respect to that portion of the Service which cannot be performed without use of the objected-to Subprocessor and provide Cleeng with notice in accordance with the MSA. Cleeng will refund a pro-rated amount covering the remainder of the term of the portion of the Services that have been terminated.

5.5 Subprocessor Agreements

Cleeng shall enter into written agreements with Subprocessors containing data protection obligations that offer at least the same level of protection as this DPA and meet the requirements of Article 28(3) of the GDPR.

6. SECURITY AND AUDIT ADDENDUM

Cleeng has implemented and maintains appropriate technical and organizational measures (TOMs) for the protection, security, confidentiality, and integrity of Customer Personal Data, considering the state of the art, costs, context, and risks to Data Subjects' rights and freedoms. Cleeng will not materially decrease the overall security during the MSA term. The specific TOMs and the terms for Customer's rights regarding Security Documentation and Audits are detailed in **Exhibit 3** **(Security and Audit Addendum)**.

7. DATA SUBJECT RIGHTS and DPIA

Cleeng shall promptly notify Customer of any Data Subject Access Request. Cleeng will assist Customer in responding to a Request by providing appropriate technical and organizational measures within the Services (e.g., export/erasure functionality), insofar as possible, for the fulfillment of Customer's obligation. Cleeng shall not respond to a Request except on Customer's documented instructions or as required by law. Cleeng will also provide reasonable assistance with data protection impact assessments (DPIAs) where required.

8. GOVERNMENT ACCESS REQUESTS

Cleeng will, where legally permitted, attempt to redirect any government, law enforcement, or regulatory request for access to Customer Personal Data directly to the Customer. If legally compelled to disclose the data, Cleeng will provide prompt and reasonable notice to Customer, take reasonable measures to challenge the terms if unable to notify, and inform Customer of its actions, unless prohibited by law. Customer is responsible for responding to all such requests.

9. PERSONAL DATA BREACH

Cleeng shall notify Customer without undue delay, and in any event no longer than forty-eight (48) hours, after becoming aware of a Personal Data Breach. Cleeng will provide Customer with the necessary information to meet its obligations under applicable Data Protection Laws (e.g., nature of the breach, data categories affected, and measures taken/proposed).

10. RETURN AND DELETION OF CUSTOMER PERSONAL DATA

Following termination of the Services, Cleeng shall:

- Provide Customer with the ability to export Customer Personal Data within thirty (30) days.
- Automatically initiate deletion of all Customer Personal Data within thirty (30) days if no written instruction is provided by the Customer.
- Complete deletion within ninety (90) days of the Cessation Date, except where retention is required by law.

Cleeng shall provide written certification of compliance upon Customer's request within four (4) months.

11. INTERNATIONAL DATA TRANSFERS

When transferring Customer Personal Data outside of the EEA, UK, or Switzerland, Cleeng relies on appropriate legal transfer mechanisms as required by Data Protection Laws and Regulations. These include:

- **Adequacy Decisions**: For transfers to countries recognized by the European Commission or other relevant authorities as providing an adequate level of data protection, such as the United Kingdom.
- **Standard Contractual Clauses (SCCs)**: For "Restricted Transfers" (transfers to countries without an adequacy decision), the transfer is subject to the applicable SCCs as detailed in Exhibit 2.

Cleeng is committed to processing Personal Data in accordance with all applicable requirements for international data transfers, including any necessary modifications for the UK and Switzerland.

12. CALIFORNIA AND U.S. STATE-SPECIFIC PROVISIONS

The Parties agree that Cleeng is a **"Service Provider"** (or equivalent) under the CPRA/CPRA and other similar U.S. State Data Protection Laws. Cleeng is prohibited from:

- Selling or Sharing Personal Data.
- Retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services.
- Retaining, using, or disclosing Personal Data for purposes outside of the Parties' direct business relationship, except as otherwise required by law.

Cleeng shall comply with the applicable obligations for a Service Provider/Processor under these laws.

13. DURATION

This DPA will remain in force for as long as Cleeng Processes Customer Personal Data on behalf of the Customer and shall automatically expire upon termination or expiration of the MSA.

14. GENERAL TERMS

14.1 Entire Agreement & Effectiveness

This DPA, including its Exhibits, is an integral part of the MSA. The DPA may be executed electronically.

14.2 Conflicts

In the event of any conflict between the MSA and this DPA, **the terms of this DPA shall prevail**. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses (SCCs), **the terms of the SCCs shall prevail**.

14.3 Limitation of Liability

The aggregate liability of the Parties arising out of this DPA is subject to the 'Limitation of Liability' section of the MSA. Nothing in this DPA shall limit the obligations of either Party with respect to a claim brought by a Data Subject directly against the Party.

14.4 Amendments

Cleeng reserves the right to amend this DPA to comply with Data Protection Laws or to reflect changes in business operations that do not materially reduce the protections provided. Cleeng will notify the Customer of material amendments, and the Customer retains the right to object in writing within fourteen (14) days.

Last Updated: 25 June, 2026

Signed by:
Gilles Domartini
5172FCBC030948F...

Gilles Domartini

CEO - Founder

26.06.2026 | 11:56 CEST

Exhibit 1: Description of Processing and Data Transfer Details

Category	Details
Data Exporter (Customer) Role	Controller
Data Importer (Cleeng) Role	Processor
Subject matter of the processing	The provision of the Subscription Services ("Services") under the MSA.
Duration of the processing	For the duration of the MSA. Data deleted/returned upon termination.
Nature and purpose of the processing	Processing as necessary to provide the functionality of the Services: managing subscriptions, authentication, payment processing, content access control, analytics, and customer support.
Categories of Data Subjects	Users (subscribers/viewers), and Customer's employees/authorized users.
Categories of Personal Data	Contact & User Data, Technical Data, Financial Data, Subscriber & Usage Data, Support Data (as detailed in DPA Section 3.1).
Special categories of data	None, unless expressly agreed in writing.
Restricted Transfers	Transfers to countries outside the EEA, UK, or Switzerland without an adequacy decision, governed by the SCCs in Exhibit 2.

Exhibit 2: Standard Contractual Clauses and Data Transfer Requirements

The Standard Contractual Clauses (SCCs), as defined in Section 1 of the DPA, are incorporated into this DPA by reference. Specifically, the Parties agree that Module Two (Controller-to-Processor) of the EU SCCs applies, with the Customer acting as the "data exporter" and Cleeng/Affiliate as the "data importer."

1. Annex I (A & B) of the SCCs is completed by the details provided in **Exhibit 1** (Description of Processing and Data Transfer Details).
2. Annex II of the SCCs is completed by the security measures detailed in **Exhibit 3** (Security and Audit Addendum).
3. The relevant provisions for the UK GDPR (via the UK International Data Transfer Addendum) and the Swiss Federal Act on Data Protection are deemed incorporated and applied to the extent required for any Restricted Transfer of Customer Personal Data.

Exhibit 3: Security and Audit Addendum

1. SECURITY MEASURES

1.1 General Security Obligations

Cleeng implements and maintains appropriate technical and organizational measures for the protection, security, confidentiality, and integrity of Customer Personal Data, considering state of the art, costs, context, and risks. Cleeng regularly monitors compliance and will not materially decrease the overall security of the Services.

1.2 Specific Security Measures

Without limiting the generality of Section 1.1, Cleeng implements the following categories of security measures:

1.2.1 Physical Access Controls

- Door locking (electric door openers, etc.)
- Securing decentralized data processing equipment and personal computers

1.2.2 Logical Access Controls

- Internal policies and procedures to grant, modify and revoke access rights
- Password policies (complexity, periodic changes, password storage)
- Multi-factor authentication for administrative access
- Automatic blocking (e.g., password-protected screen saver)
- Encryption of data carriers
- Use of certified security products
- Logging of access to applications and systems
- Intrusion detection and intrusion prevention systems
- Network segmentation and isolation
- Regular access reviews and recertification

1.2.3 Data Access Controls

- Internal policies and procedures for granting, modifying, and revoking data access permissions

- Role-based access control (RBAC) mechanisms
- Attribute-based access control where appropriate
- Principle of least privilege enforcement
- Segregation of duties for critical functions
- Access logging and monitoring
- Regular review of access rights
- Data classification and handling procedures

1.2.4 Transmission Controls

- Encryption of data during transmission using industry-standard protocols (TLS 1.2 or higher)
- Virtual Private Networks (VPNs) for remote access
- Encryption/tunneling for Wide Area Network (WAN) connections
- Logging of data transmission activities
- Data leakage prevention measures
- Secure file transfer protocols

1.2.5 Input Controls

- Procedures and technical measures to determine whether and by whom Personal Data has been entered, modified or removed from data processing systems
- Audit logging and trail mechanisms
- Version control and change management systems
- User activity monitoring
- Document management systems with versioning

1.2.6 Data Availability Controls

- Backup procedures and disaster recovery plan
- Uninterruptible power supply (UPS)
- Remote storage of backup media

- Regular testing of backup and recovery procedures
- Antivirus/anti-malware software
- Firewalls and network security devices
- Business continuity and incident response plans
- Redundant systems and failover capabilities
- Regular patching and vulnerability management

1.2.7 Data Separation Controls

- Physical or logical separation of data collected for different purposes
- Multi-tenancy architecture with proper isolation
- Database-level separation where appropriate
- "Separation of production and test systems" procedures
- Test data management and anonymization procedures

1.2.8 Data Integrity Controls

- Checksums and hash functions to verify data integrity
- Data validation at input and processing stages
- Integrity monitoring systems
- Change detection mechanisms
- Audit trails for data modifications

1.3 Security Certifications and Standards

Cleeng maintains third-party certifications, including **SOC 2 Type 2 certification** and other applicable security certifications as maintained by Cleeng. These certifications and related audit reports constitute the "Security Documentation."

1.4 Personnel Security

- Background checks for personnel with access to Customer Personal Data (where permitted by law)
- Confidentiality agreements executed by all personnel
- Regular security awareness training

- Clear definition of security roles and responsibilities
- Procedures for personnel termination and access revocation

1.5 Vendor and Third-Party Management

- Security assessments of Subprocessors and vendors
- Contractual security requirements for third parties
- Regular review of third-party security posture
- Incident notification requirements for third parties

1.6 Application Security

- Secure software development lifecycle (SDLC)
- Code reviews and security testing
- Regular security assessments and penetration testing
- Vulnerability scanning and management
- Web application firewalls (WAF)
- API security controls
- Input validation and output encoding
- Protection against common vulnerabilities (OWASP Top 10)

1.7 Incident Response and Management

- Documented incident response plan
- Designated incident response team
- Incident detection and monitoring systems
- Incident classification and escalation procedures
- Post-incident review and lessons learned processes

1.8 Security Governance

- Information security policies and procedures
- Security risk assessment program

- Security metrics and reporting
- Regular management review of security posture
- Continuous improvement processes

1.9 Availability of Security Information

Detailed technical and organizational security measures are available upon request to existing customers under appropriate confidentiality obligations. Such information may include:

- Detailed descriptions of security controls
- Architecture and infrastructure security documentation
- Compliance and certification reports
- Risk assessment summaries

2. SECURITY DOCUMENTATION AND AUDITS

2.1 Security Documentation

Upon Customer's written request at reasonable intervals (no more than once per year unless required by regulatory authorities or following a Personal Data Breach), Cleeng will make available to the Customer or its Third-Party Auditor a copy of its Security Documentation to enable Customer to undertake a risk-based assessment of Cleeng's compliance with this DPA.

Security Documentation may be shared with Customer's competent Supervisory Authority. Customer acknowledges that the Security Documentation is Confidential Information of Cleeng and/or its Subprocessors and must be treated accordingly.

2.2 Acceptance of Security Documentation

Cleeng requests that Customer accept the Security Documentation in place of an Audit other than where Customer has reasonable belief that Cleeng is in breach of this DPA.

If the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2 or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Cleeng has confirmed there are no known material changes in the controls audited, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures.

2.3 Audits

Where Customer has reasonable belief that Cleeng is in breach of this DPA, Customer may contact Cleeng to request an audit of the Processing activities covered by this DPA ("Audit"). An Audit may be conducted by Customer either itself or through a Third-Party Auditor selected by Customer when:

(i) The information made available to Customer by Cleeng under Section 2.1 is not sufficient to evidence compliance with this DPA as determined by Customer acting reasonably;

(ii) Customer received a notice of a Personal Data Breach;

(iii) If required under Data Protection Laws and Regulations; or

(iv) Upon request of Customer's competent Supervisory Authority

Customer agrees that any Audit conducted will be reasonable, requested in good faith, and proportional to the Services provided (taking into account the nature and complexity thereof).

2.4 Audit Procedures

An Audit may occur up to one time (1x) per year upon Customer providing Cleeng with at least thirty (30) days advance written notice, except where Customer is relying on circumstances (ii) or (iv) above, in which case shorter notice periods may apply.

All Audits will be:

- Scheduled by Cleeng to take place during its normal business hours
- Conducted for a reasonable duration
- Limited to the audit of architecture, systems and procedures relevant to the processing of Personal Data
- Structured to not interfere with Cleeng's day-to-day operations

Before an Audit commences, Customer and Cleeng shall mutually agree upon:

- The scope, timing, and duration of the Audit
- The reimbursement rate for which Customer shall be responsible

All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Cleeng. Cleeng agrees that reasonable costs of an Audit undertaken by Customer or its Third-Party Auditor following notice of a Personal Data Breach shall be for Cleeng to pay.

2.5 Third-Party Auditors

An Audit may be conducted through a Third-Party Auditor if:

(i) Prior to the Audit, the Third-Party Auditor enters into a non-disclosure agreement with Cleeng that contains confidentiality provisions no less protective of Cleeng's information than those set forth in the MSA;

(ii) All Third-Party Auditor costs are at Customer's expense (except as provided in Section 2.4); and

(iii) The Third-Party Auditor is not a competitor of Cleeng and produces reasonable evidence of identity and authority

2.6 Audit Results

Customer agrees to promptly provide Cleeng with information regarding any non-compliance discovered during an Audit. The Parties shall make the information and results of any audits available to the competent Supervisory Authority on request.

2.7 Subprocessor Audits

Should Customer seek to conduct an audit or inspection of a non-Affiliate Subprocessor, Cleeng will use commercially reasonable efforts to facilitate such a request.