Data Processing Agreement

SMTP.dk and mySMTP

Template under Article 28(3) of the GDPR

This Agreement governs the processing of personal data by SMTP.dk ApS when providing SMTP email relay services to the customer. Annexes A to D describe the processing, subprocessors, instructions, security measures and related matters.

English version of the template dated 22 November 2026. Complete the customer-specific fields when entering into the Agreement.

Parties

Controller

Customer’s legal name

Company registration number

Registered address and country

Processor

SMTP.dk ApS
Danish company registration number (CVR) 29849439
Refshalevej 163A
1432 Copenhagen K
Denmark

Each a Party and together the Parties.

The Parties agree to the following data processing provisions (the Provisions) to comply with the GDPR and protect the privacy and fundamental rights and freedoms of natural persons.

References to Member States include EEA Member States.

1 Contents

Sections 2 to 15 contain the Provisions. Annex A describes the processing. Annex B lists subprocessors. Annex C sets out instructions and security measures. Annex D covers other matters.

2 Preamble

2.1 These Provisions set out the Processor’s rights and obligations when processing personal data on behalf of the Controller.

2.2 These Provisions are intended to ensure compliance with Article 28(3) of Regulation (EU) 2016/679 (GDPR).

2.3 The Processor processes personal data on behalf of the Controller in accordance with these Provisions when providing SMTP email relay under the SMTP.dk and mySMTP names.

2.4 These Provisions take precedence over corresponding terms in other agreements between the Parties.

2.5 Annexes A to D form an integral part of these Provisions.

2.6 Annex A specifies the purpose, nature and duration of processing, the types of personal data and the categories of data subjects.

2.7 Annex B specifies the conditions for engaging subprocessors and lists the subprocessors the Controller has authorised.

2.8 Annex C specifies the Controller's instructions, minimum security measures and arrangements for oversight of the Processor and its subprocessors.

2.9 Annex D addresses other activities outside the scope of these Provisions.

2.10 Both Parties shall retain these Provisions and their Annexes in writing, including in electronic form.

2.11 The Processor remains subject to its obligations under the GDPR and other applicable law.

3 Rights and obligations of the Controller

3.1 The Controller is responsible for ensuring that processing complies with the GDPR, including Article 24, applicable EU and Member State data protection law and these Provisions.

3.2 The Controller has the right and obligation to determine the purposes and means of processing.

3.3 The Controller is responsible for ensuring a lawful basis for the processing it instructs the Processor to perform.

4 Documented instructions

4.1 The Processor shall process personal data only on documented instructions from the Controller, unless required by applicable EU or Member State law. Annexes A and C set out these instructions. The Controller may issue further instructions during processing. The Parties shall document and retain them with these Provisions in writing, including electronically.

4.2 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable EU or Member State data protection law.

5 Confidentiality

5.1 The Processor shall restrict access to personal data to persons acting under its authority who have undertaken confidentiality or are subject to an appropriate statutory duty of confidentiality. Access shall be limited to what is necessary. The Processor shall regularly review granted access and revoke access once it is no longer needed.

5.2 At the Controller's request, the Processor shall demonstrate that authorised persons are subject to the required confidentiality duties.

6 Security of processing

6.1 Under Article 32 GDPR, both Parties shall implement technical and organisational measures appropriate to the risk, taking account of the state of the art, implementation costs and the nature, scope, context and purposes of processing, as well as the likelihood and severity of risks to individuals.

The Controller shall assess risks to individuals' rights and freedoms and take measures appropriate to those risks. Where relevant, these may include the following.

a) Pseudonymisation and encryption of personal data.

b) The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.

c) The ability to restore availability and access to personal data in a timely manner after a physical or technical incident.

d) Regular testing, assessment and evaluation of the effectiveness of security measures.

6.2 The Processor shall independently assess the risks to individuals and implement appropriate measures under Article 32. The Controller shall provide the information necessary for that assessment.

6.3 The Processor shall assist the Controller with its obligations under Article 32 by providing information about measures already in place and any other information necessary for the Controller's compliance.

If the Controller's risk assessment requires additional measures, the Controller shall specify them in Annex C.

7 Use of subprocessors

7.1 The Processor shall comply with Article 28(2) and (4) GDPR when engaging a subprocessor.

7.2 The Processor shall obtain prior general written authorisation from the Controller before engaging a subprocessor under these Provisions.

7.3 The Controller gives general written authorisation. The Processor shall give at least 30 days' prior written notice of any intended addition or replacement so the Controller can object before engagement. Annex B may specify longer notice for particular activities and lists the subprocessors already authorised.

7.4 The Processor shall impose the same data protection obligations on each subprocessor by contract or other binding legal act under EU or Member State law. This shall include sufficient guarantees that appropriate technical and organisational measures will be implemented.

The Processor shall require the subprocessor to meet at least the data protection obligations applicable to the Processor under these Provisions and the GDPR.

7.5 On request, the Processor shall provide the Controller with copies of subprocessor agreements and amendments. Commercial terms unrelated to data protection may be withheld.

7.6 The Processor remains fully liable to the Controller for its subprocessors' compliance. The rights of data subjects, including under Articles 79 and 82 GDPR, remain applicable.

8 Transfers to third countries or international organisations

8.1 The Processor may transfer personal data to a third country or international organisation only on documented instructions and in compliance with Chapter V GDPR.

8.2 If applicable EU or Member State law requires an otherwise uninstructed transfer, the Processor shall inform the Controller before processing unless that law prohibits notice on important grounds of public interest.

8.3 Documented instructions are required for each of the following activities under these Provisions.

a) Transferring personal data to a controller or processor in a third country or to an international organisation.

b) Entrusting processing to a subprocessor in a third country.

c) Processing personal data in a third country.

8.4 Annex C.6 shall record the Controller's transfer instructions and the applicable Chapter V transfer basis.

8.5 A separate Chapter V transfer basis is required where applicable. These Provisions are entered into under Article 28 GDPR.

9 Assistance to the Controller

9.1 Taking account of the nature of processing, the Processor shall assist the Controller, as far as possible, through appropriate technical and organisational measures in responding to requests under Chapter III GDPR.

This assistance covers the following obligations and rights.

a) Providing information when personal data are collected from the data subject.

b) Providing information when personal data are obtained from other sources.

c) The right of access.

d) The right to rectification.

e) The right to erasure.

f) The right to restriction of processing.

g) Notification obligations concerning rectification, erasure or restriction of processing.

h) The right to data portability.

i) The right to object.

j) Rights concerning decisions based solely on automated processing, including profiling.

9.2 In addition to clause 6.3, the Processor shall assist the Controller with the following, taking account of the nature of processing and information available to the Processor.

a) Notifying the competent supervisory authority of a personal data breach without undue delay and, where feasible, within 72 hours of awareness, unless the breach is unlikely to pose a risk to individuals' rights and freedoms.

b) Communicating a personal data breach to affected data subjects without undue delay when it is likely to result in a high risk to their rights and freedoms.

c) Carrying out a data protection impact assessment before the proposed processing.

d) Consulting the competent supervisory authority before processing where the impact assessment indicates a high risk in the absence of measures to mitigate it.

9.3 Annex C specifies the technical and organisational measures and the scope of assistance under clauses 9.1 and 9.2.

10 Personal data breach notification

10.1 The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach.

10.2 Where feasible, notification shall take place within 24 hours of awareness so the Controller can meet its obligations under Article 33 GDPR.

10.3 Under clause 9.2(a), the Processor shall assist the Controller in notifying the competent supervisory authority and provide the information required by Article 33(3), as available.

a) The nature of the breach and, where possible, the categories and approximate numbers of data subjects and personal data records affected.

b) The likely consequences of the breach.

c) The measures taken or proposed by the Controller to address the breach, including measures to mitigate adverse effects where relevant.

10.4 Annex C specifies the information the Processor shall provide to support the Controller's notification.

11 Deletion and return of personal data

11.1 When the processing services end, the Processor shall, at the Controller's choice, delete or return all personal data processed on its behalf and delete existing copies, unless EU or Member State law requires retention. The Processor shall confirm deletion. Annex C.4 sets out the procedure.

Where retention is required by law, the Processor shall process the data only for the purposes, period and under the conditions prescribed by that law.

12 Audits and inspections

12.1 The Processor shall make available all information necessary to demonstrate compliance with Article 28 GDPR and these Provisions and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller.

12.2 Annexes C.7 and C.8 set out the procedures for audits and inspections of the Processor and its subprocessors.

12.3 The Processor shall grant access to its physical premises to supervisory authorities and their representatives entitled to access under applicable law, upon presentation of appropriate identification.

13 Other terms

13.1 The Parties may agree other terms for the services, including on liability, provided these terms are consistent with these Provisions and preserve data subjects' fundamental rights and freedoms.

14 Entry into force and termination

14.1 These Provisions take effect when both Parties have signed.

14.2 Either Party may request renegotiation if changes in law or shortcomings in these Provisions warrant it.

14.3 These Provisions apply throughout the processing services. They may be terminated during that period only if the Parties agree replacement terms governing those services.

14.4 After the services end and the personal data have been deleted or returned under clause 11.1 and Annex C.4, either Party may terminate these Provisions by written notice.

14.5 Signatures

Controller	Processor
Name _____ Title _____ Date _____ Signature _____	Name _____ Title _____ Date _____ Signature _____

15 Contact persons

15.1 The Parties may contact each other through the contacts below.

15.2 Each Party shall keep the other informed of changes to its contacts.

Contact	Controller	Processor
Name and role		
Operations and breach email		
Urgent contact telephone		

Annex A. Details of processing

A.1 Purpose

The purpose is to relay the Controller’s emails to its designated recipients and support delivery, troubleshooting, operation and security of the service.

Customer’s specific purposes and email types

A.2 Nature of processing

SMTP.dk/mySMTP receives customer-prepared emails and forwards them to the specified recipients’ mail servers. SMTP.dk does not edit message content or customise customer headers. Transport and authentication can add technical headers, including transport information and DKIM signatures. SPF, DKIM and DMARC form part of the service configuration for the agreed sending domains. Connections follow the service’s TLS policy. Emails are not stored in an outbound queue. If delivery fails, the sender receives an error response or a bounce notice. Transaction and delivery logs are available for up to 30 days from the original transaction and are then deleted. Authorised support personnel may access information as necessary within the instructions.

A.3 Types of personal data

Processing covers sender and recipient addresses, personal data in headers, subjects, message content and attachments, and relevant transaction information such as timestamps, IP addresses, message identifiers, delivery status and SMTP errors.

Customer's specific categories of personal data

Processing special categories of data under Article 9 GDPR, criminal offence data under Article 10 or Danish CPR numbers requires a separate written agreement specifying the categories and additional safeguards before processing.

A.4 Categories of data subjects

Senders, recipients and other people referred to in customer emails. Depending on the customer's use, this may include customers, users, participants, employees and business contacts.

Customer's specific categories of data subjects

A.5 Duration

Processing starts once the Agreement takes effect and continues during the service. Email content is processed for the period needed to transmit the message. Emails are not stored in an outbound queue. Logs are available for up to 30 days from the original email transaction and then deleted, including copies and backups. Annex C.4 governs other deletion procedures. The Agreement applies until the data have been deleted or returned.

Annex B. Subprocessors

B.1 Authorised subprocessors

Name and registration	Address	Processing
AdeoDC CVR 37593184	Herstedvang 8 2620 Albertslund Denmark	Hosting of the SMTP platform in Denmark.
Expertlance / Radu Milcoveanu RO51704680	Bulevardul Iuliu Maniu 7 Corp T061072 Bucharest Romania	Development and support of the SMTP platform in Romania.

When the Agreement takes effect, the Controller authorises the subprocessors listed above for the stated activities and locations within the agreed instructions.

B.2 Changes and notice

General written authorisation applies under clauses 7.2 and 7.3. The Processor shall give at least 30 days' written notice before adding or replacing a subprocessor. The notice shall identify the supplier, activity, processing countries, relevant access arrangements and any changes to the transfer basis.

The Controller may object before engagement. The Parties shall resolve a timely objection before entrusting the affected processing to the new subprocessor. Extensions to activities or locations require written approval under Annex C.5.

B.3 Self-hosted WHMCS customer platform

SMTP.dk self-hosts WHMCS and uses it for customer administration, products, subscriptions and billing in its capacity as controller under Annex D.2. The software licence alone gives WHMCS.com no subprocessor role. Any separate supplier support access to data processed on the customer's behalf shall be assessed and governed before access is granted.

Annex C. Instructions and security measures

C.1 Subject matter and instructions

The customer submits emails to SMTP.dk, which forwards them to the customer's designated recipients. Emails are not stored in an outbound queue. If an email cannot be sent, the sender receives an error response or a bounce notice. Transaction details and logs are used for operational monitoring and troubleshooting and deleted under Annex C.4.

The instructions cover the agreed email service and necessary operation, security and support. Any further use of customer data requires a separate lawful basis and clear allocation of roles.

Direct customer relationship

The customer is the Controller, SMTP.dk is the Processor and the suppliers in Annex B are subprocessors. The customer's system submits the email to SMTP.dk, which delivers it to the recipient's mail server.

Customer acting as processor

Where the customer sends on behalf of another controller, the customer acts as processor, SMTP.dk acts as a subprocessor and the suppliers in Annex B act as further subprocessors. The customer shall obtain the required authorisation and ensure that its instructions and this Agreement reflect its obligations to the original controller. The Parties shall adapt the role descriptions when entering into the Agreement.

C.2 Security of processing

The security level shall reflect the nature, scope, context and purpose of processing and the risks to data subjects. The Processor shall select and maintain appropriate technical and organisational measures. All covered information shall be handled with a high degree of confidentiality.

Risk management and policies

Risk management shall be based on a documented, regularly updated assessment of risks to data subjects and the processing activities. Management shall review and approve security policies and procedures at least annually. Relevant policies and procedures shall be provided on request.

Development and change management

Documented development and change procedures shall apply data protection by design and by default. Critical network access points shall be protected and systems regularly tested for vulnerabilities.

Identity and access

Each employee or other person with access shall be assigned a unique individual account. Access shall be limited to what is necessary, approved by an authorised person, recorded, regularly reviewed and revoked once no longer needed.

Passwords and remote access

The employee password policy shall be reviewed at least annually. Passwords shall contain at least 12 characters, including upper- and lower-case letters, numbers and special characters. Customers shall receive an automatically generated password at first login. Remote access shall use encrypted connections and two-factor authentication.

Confidentiality and training

Employees shall be bound by written confidentiality obligations during and after employment. Relevant personnel shall receive training at least annually on the GDPR, internal security and data protection policies, and social engineering awareness.

Workstations and portable media

Unattended workstations shall be locked and physical records secured. Local storage on laptops, phones, USB media or external drives requires a specific agreement with the customer. Access from mobile devices requires two-factor authentication.

Networks and endpoints

Firewalls and antivirus protection shall be used. Network access shall be restricted. Relevant systems shall be maintained and updated under documented procedures. Vulnerabilities shall be assessed and addressed according to risk.

Logging

Access events and significant system and key events shall be logged. Logs shall be protected and available to authorised personnel for oversight, troubleshooting and incident response, and deleted under Annex C.4.

Secure exchange and email transport

Administrative data exchange shall primarily use SSH. If that is unavailable, email with enforced end-to-end encryption may be used with the customer's approval. This requirement applies to administrative exchanges.

Physical security

Servers and other processing equipment shall be kept in locked premises. Server rooms shall be protected against fire and theft. The Processor's premises and relevant physical media shall be protected against unauthorised access.

Backup and recovery

Log backups are subject to the same maximum age of 30 days from the original email transaction. Recovery procedures shall be documented and tested.

Incident handling and controls

The Processor shall maintain procedures to prevent, detect, classify and respond to personal data breaches and notify the customer. Breach procedures shall be tested at least annually. Data loss prevention processes and policies shall be evaluated at least annually. Deviations shall be addressed through documented corrective actions and follow-up.

The SMTP service uses transport encryption where TLS is supported and established. Any requirement for mandatory TLS or end-to-end encryption on customer relay traffic must be agreed in writing before the relevant processing.

C.3 Assistance to the Controller

Taking account of the nature of processing and available information, the Processor shall assist with identification, extraction, restriction, deletion and return of relevant data. Requests received directly from data subjects about customer processing shall be forwarded without undue delay. The Processor shall respond directly only where instructed or legally required.

The Processor shall provide information on processing activities, data flows and safeguards for risk assessments, impact assessments and prior consultation, and guidance on agreed secure communication channels.

The Processor shall give initial breach notice without undue delay and, where feasible, within 24 hours of awareness. The notice shall include available details about the nature and timing of the breach, affected systems and data, approximate numbers of data subjects and records, likely consequences, action taken or planned and the contact person. Further information shall follow as available. The Controller decides on regulatory and data subject notification.

C.4 Retention and deletion

Information	Retention and deletion
Email content and attachments	Processed as necessary for transmission. Emails are not stored in an outbound queue. If delivery fails, the sender receives an error response or a bounce notice.
Transaction details and delivery logs	Available for up to 30 days from the original email transaction. The data and copies are then deleted.
Log backups	Maximum age of 30 days from the original email transaction. Backups do not extend the retention period.
Other logs containing customer data	Logs covered by this Agreement are deleted within 30 days of the recorded event.
Support cases containing customer relay data	Copies of relay logs are subject to the same 30-day limit from the original transaction. Data covered by this Agreement may be shared with an external support system only if the supplier is authorised under Annex B.

Upon termination the default instruction is deletion with confirmation under clause 11.1. The customer may request return in writing before deletion, followed by deletion of existing copies. Previously lawfully deleted data shall not be recreated for return.

Deletion covers all remaining data and existing copies. Backups shall not retain logs beyond 30 days from the original email transaction. Restoration shall not reintroduce data due for deletion. The Processor shall confirm completion.

Where EU or Member State law requires further retention, the Processor shall inform the customer of the legal basis, scope and duration unless notification is prohibited. Retained data shall be used solely for that legal purpose.

C.5 Processing locations

AdeoDC hosts the SMTP platform at Herstedvang 8, 2620 Albertslund, Denmark. Expertlance provides development and support from the Romanian location in Annex B. SMTP.dk processes data from its stated premises and separately approved remote workplaces.

Processing or access from other locations requires prior written customer approval. Authorisation of a new subprocessor is separate from any required third-country transfer instruction under Annex C.6.

C.6 Third-country transfer instructions

Transfers to and access from third countries are governed by clause 8. This Agreement grants no general authorisation for new third-country transfers. Where Chapter V applies, any transfer must be covered by documented instructions and a valid transfer basis.

Any third-country processing requires specific documented instructions and a valid transfer basis where Chapter V applies.

C.7 Customer oversight of SMTP.dk

For routine oversight, the Controller sends SMTP.dk a GDPR questionnaire. At least annually, SMTP.dk shall answer relevant questions at no extra charge and provide supporting documentation without undue delay or within a reasonable agreed period. The Controller may request further information under clause 12.

SMTP.dk does not hold an ISAE assurance report. The questionnaire process preserves the Controller’s audit and inspection rights under clause 12 and both Parties’ mandatory obligations.

The customer or its mandated auditor may conduct necessary audits and inspections, including on-site inspections. Scheduling shall take reasonable account of operations, confidentiality and other customers’ data.

Notice requirements shall allow necessary checks following incidents, reasonable suspicion or regulatory requirements.

SMTP.dk shall make resources available for oversight, remedy documented deviations and follow up. The customer may request necessary evidence and safeguards. Supplier documentation may supplement evidence of SMTP.dk's own controls.

C.8 Oversight of subprocessors

SMTP.dk shall document its oversight of authorised subprocessors at least annually and after material changes or incidents. Oversight shall reflect the activity and risk and cover agreements, access, locations, security, deletion and remediation.

Oversight shall draw on written information, questionnaires and evidence of actual controls. Standard assurance materials may be used where available. SMTP.dk shall follow up on inadequate evidence and perform further checks as necessary. A specific ISAE report is not generally required.

SMTP.dk shall provide relevant oversight evidence, follow up on shortcomings and secure contractual rights for necessary checks. The customer may request additional checks and participate in inspections where necessary. SMTP.dk remains responsible under clause 7.

Annex D. Other matters

D.1 Relationship with the service agreement

Pricing, subscriptions, support and other commercial terms are governed by the service agreement to the extent consistent with these Provisions and data subjects' rights. This Annex imposes no separate limitation of liability.

D.2 Processing outside these instructions

SMTP.dk may process information as an independent controller for purposes such as billing, accounting and customer administration. Its relevant privacy information describes these purposes, lawful bases and retention periods. The role depends on the actual processing.

SMTP.dk self-hosts WHMCS for products, subscriptions and billing as controller. Retention for billing and customer administration follows the applicable purposes and statutory requirements.

WHMCS.com supplies the software. Any external supplier access to personal data for support or other processing requires the parties to establish the applicable roles and agreements before access.

D.3 Potentially unlawful instructions

If SMTP.dk considers an instruction unlawful under clause 4.2, it shall promptly inform the customer and explain its reasons. SMTP.dk may suspend the affected processing where necessary while the Parties establish a lawful instruction. The Parties' other obligations continue to apply.