DATA PROCESSING AGREEMENT

SEPTEMBER 2026

Based on the Danish Data Protection Authority's official standard template.

Agillic A/S
Masnedøgade 22
2100 Copenhagen Ø
Denmark

contact@agillic.com
www.agillic.com

1. Table of contents

By signing an Agillic Order Form, the Customer as the “data controller” and Agillic A/S as the “data processor”, each a ‘party’, together ‘the Parties’, have agreed to the following contractual clauses (the “Clauses”) in order to meet the requirements of The General Data Protection Regulation (“GDPR”) and to ensure the protection of the rights of the data subject.

2. PREAMBLE

2.1. The Clauses set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

2.3. In the context of the provision of **The Agillic Omnichannel Marketing Automation Platform (the "Platform")**, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

2.6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

2.8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

2.9. Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the GDPR or other legislation.

3. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

3.1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

3.2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

4.1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. CONFIDENTIALITY

5.1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. SECURITY OF PROCESSING

6.1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures 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 the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

6.3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. USE OF SUB-PROCESSORS

7.1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

7.2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior:

Choice 1: specific written authorisation.

Choice 2: general written authorisation of the data controller.

Choice 1 or 2 is specified in the Order Form.

7.3. [OPTION 1 SPECIFIC PRIOR AUTHORISATION] The data processor shall engage sub-processors solely with the specific prior authorisation of the data controller. The data processor shall submit the request for specific authorisation at least 30 days prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the data controller can be found in Appendix B.

[OPTION 2 GENERAL WRITTEN AUTHORISATION] The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

7.5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

7.6. In the event of bankruptcy of the data processor sub-processors are instructed to delete all data. Data cannot be returned as it is encrypted and impossible for the sub-processor to decrypt and pseudonymised and the sub-processor does not know who the data controller is.

7.7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

8.1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

8.2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

a) transfer personal data to a data controller or a data processor in a third country or in an international organisation;

b) transfer the processing of personal data to a sub-processor in a third country;

c) have the personal data processed in by the data processor in a third country.

8.4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

8.5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. ASSISTANCE TO THE DATA CONTROLLER

9.1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a) the right to be informed when collecting personal data from the data subject

b) the right to be informed when personal data have not been obtained from the data subject

c) the right of access by the data subject;

d) the right to rectification

e) the right to erasure ('the right to be forgotten')

f) the right to restriction of processing

g) notification obligation regarding rectification or erasure of personal data or restriction of processing

h) the right to data portability

i) the right to object

j) the right not to be subject to a decision based solely on automated processing, including profiling

9.2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3, the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a) the data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Datatilsynet, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b) the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c) the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d) the data controller's obligation to consult the competent supervisory authority, Datatilsynet, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

9.3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. NOTIFICATION OF PERSONAL DATA BREACH

10.1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

10.2. The data processor's notification to the data controller shall, if possible, take place within **24 hours** after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

10.3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) the likely consequences of the personal data breach;

c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. ERASURE AND RETURN OF DATA

11.1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so.

11.2. The following EU or Member State law applicable to the data processor requires storage of the personal data after the termination of the provision of personal data processing services:

a) Denmark

The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

12. AUDIT AND INSPECTION

12.1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

12.2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

12.3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. THE PARTIES' AGREEMENT ON OTHER TERMS

13.1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. COMMENCEMENT AND TERMINATION

14.1. The Clauses shall become effective on the date of both parties' signature.

14.2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

14.4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

14.5. Signature: See Order Form.

15. DATA CONTROLLER AND DATA PROCESSOR CONTACTS/CONTACT POINTS

15.1. The parties may contact each other using the following contacts/contact points:

The data processor: https://agillic.com/company/contact/

The data controller: See Order Form.

15.2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

APPENDIX A – INFORMATION ABOUT THE PROCESSING

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

To allow the data controller to send communications to recipients based on personal data provided by the data controller using the Platform provided by the data processor.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Storing, generation, and delivery of personalised communication e.g. via email, pdf, SMS, app notifications to specific individual recipients and target groups on third party media platforms.

A.3. The processing includes the following types of personal data about data subjects:

See specification in the Order Form

A.4. Processing includes the following categories of data subject:

See specification in the Order Form

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Until deletion by the data controller, which can be done at any time, or 30 days after the end of contract between the data controller and data processor.

APPENDIX B – AUTHORISED SUB-PROCESSORS

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

See specification in the Order Form

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

At least 30 days.

APPENDIX C – INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

Storing, generation, and delivery of personalised communication e.g. via email, pdf, SMS, app notifications, third party media platforms to specific recipients and target groups.

C.2. Security of processing

The level of security shall take into account:

That the processing involves a large volume of personal data as specified by the data controller in the Order Form.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

IT security policy
Agillic has in place an IT security policy, which all employees must comply with. The IT security policy is part of the onboarding process that new employees are being introduced to and an annual awareness training for all employees.

Risk assessment
Agillic has a structured risk assessment process in place that takes into consideration possible privacy impacts related to the transfer of data.

Anti-virus
All Agillic workstations are equipped with an anti-virus program.

Network segmentation and firewall
Agillic networks and VPN connections are segmented to the effect that unrelated servers cannot communicate directly with each other. A firewall is placed on top of the networks. The network in the office is segmented in two networks; there is a WiFi-network for employees and one for guests. The guest network cannot access any internal systems.

User creation
A user is created when a new person is hired as part of the onboarding process. The privileges of the user are determined prior to the onboarding process according to the specific job function.

User termination
Upon termination of a user, it is first assessed whether the accounts contain information that Agillic might need in the future. If the user accounts are assessed as not containing information needed by Agillic in the future, the accounts and data are removed. If the user accounts are assessed as containing information needed by Agillic in the future, the accounts have their passwords reset, and

the accounts are locked to ensure that there is no access to the user until needed. An offboarding document is created where the removal of certain access, accounts, etc. is documented.

Privileged access rights
Privileges are documented in the onboarding document and can be cross-checked at any given time. Privileged access is only granted if an employee needs it to perform their job function.

System monitoring
All servers have a monitoring agent that sends data to an alerting system to create alarms that are monitored 24/7 by humans with automatic escalation procedures.

Encryption
All communication from the frontend to the backend is encrypted using min. TLS 1.2.

Logging
All systems are logged, and the logs are sent to a separate server for handling except for certain low-risk systems, where logs are kept locally.

Change management
All releases are going through a change management process where the changes are approved by a qualified engineer with proper training.

Data in use
To the highest degree feasible, data in at rest or in transit must be secured by one of the following actions:

- Hashing
- Encryption
- Pseudonymisation

Vulnerability and penetration scans
All Customer-faced servers are scanned on a regular basis. The results are documented and vulnerabilities are assessed and handled by the responsible system owner.

Security patching
Agillic systems are upgraded on a regular basis. In the event of a new-found vulnerability with an attached CVE, the systems are manually patched as soon as possible.

Two-factor authentication
Agillic enforces two-factor (2FA) authentication on internal access to Customers' data and provides Customers with the option to enable 2FA on the Agillic Platform.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Technical measures are described in C.2 and the data processor will provide necessary personnel to provide information described in Clause 9.1. and 9.2.

C.4. Storage period/erasure procedures

Personal data is stored until 30 days after the end of contract between the data controller and data processor after which the personal data is automatically erased by the data processor.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Locations inside the EU or The European Commission has determined to offer an adequate level of data protection.

C.6. Instruction on the transfer of personal data to third countries

Customers can actively choose to use connectors in the platform and thereby instruct the data processor to transfer personal data to a third country or international organisation for which the Customer has confirmed to have a GDPR valid legal basis.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall annually at THE DATA PROCESSOR'S expense obtain an INSPECTION REPORT from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of INSPECTION REPORT may be used in compliance with the Clauses: ISAE 3000

The INSPECTION REPORT shall without undue delay be submitted to the data controller for information upon request. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required.

APPENDIX D – THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS

See Order Form.