AMC BANKING

Data Processing Agreement

Content

The Parties

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR).

1.1 The Data Processor

Company Name:	AMC Consult A/S
CVR:	16987344
Address:	Grundtvigsvej 29, 1864 Frederiksberg Denmark
Name and title of signee:	Peter Makki, CEO
Signature:	

1.2 The Data Controller

Company Name: _____

CVR: _____

Address: _____

Date: _____

Name and title of signee: _____

Signature: _____

each a 'party'; together 'the Parties'

have agreed on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

2 PREAMBLE

1. These Contractual Clauses (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. The following data processing agreement shall be an addendum to and form part of the agreements governing the relationship between Data Controller and Data Processor (the Agreements), namely:

   - Data Processing Agreement (DPA)
   - End user license agreement (EULA)
   - Service level agreement (SLA)
   - Non-Disclosure Agreement (NDA)
   - General terms and conditions for the supply of software and consultancy services (Terms)

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).

3. In the context of the maintenance and provision of the AMC Banking products and services, the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.

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

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

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.

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.

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.

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

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

11. The Clauses shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3 THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

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.

2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

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

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 Data 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.

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.

3. The Data Processor shall give notice without undue delay if the Data Processor considers an instruction to conflict with the Applicable Law.

5 CONFIDENTIALITY

---

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

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.

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

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 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.

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.

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 require 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

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).

2. The Data Processor shall therefore not engage with Sub-Processors for the fulfilment of the Clauses without the prior general written authorisation of the Data Controller.

3. 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 1 month 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.

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.

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.

6. The Data Processor shall agree a third-party beneficiary clause with the Sub-Processor where – in the event of bankruptcy of the Data Processor – the Data Controller shall be a third-party beneficiary to the Sub-Processor agreement and shall have the right to enforce the agreement against the Sub-Processor engaged by the Data Processor, e.g. enabling the Data Controller to instruct the Sub-Processor to delete or return the personal data.

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

8. 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

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.

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.

   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 organization

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

3. 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.

4. 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

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.

1. 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, 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 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.

1.	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

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.

2.	The Data Processor's notification to the Data Controller shall, if possible, take place within 48 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.

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 Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

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 unless Union or Member State law requires storage of the personal data.

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:

- Act on Measures to Prevent Money Laundering and Financing of Terrorism.

    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

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.

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.

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

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

1. The Clauses shall become effective on the date of the Parties' signatures.

2. The 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.

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.

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.

APPENDIX A: INFORMATION ABOUT PROCESSING

A.1. The purpose of the processing of personal data on behalf of the Data Controller

AMC needs to process certain personal data for the following purposes:

- To establish a license for an AMC Banking product in accordance with the contractual obligations.
- To offer support to the Data Controller and the end user of AMC's services.
- To develop the quality and functionality of AMC's services.
- To process orders, invoicing, payments and other financial activities.
- To perform the services included in AMC Products.
- To ensure compliance with Act on Measures to Prevent Money Laundering and Financing of Terrorism.
- To ensure security for money transfers.
- To offer transparency to the customer.
- To offer fraud detection algorithms.

A.2. The processing of personal data on behalf of the Data Controller shall mainly pertain to

The Data Processor makes software services available to the Data Controller and thereby process personal data, primarily personal data of the 'end users', as engaged by the Data Controller or other personal data added by the Data Controller or it's end users, vendors and customers, always subject to the limitations set out in A.5.

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

- Name
- Company
- Title
- Phone number
- E-mail
- Address
- Bank account number (only for personal bank transfers)
- IP-address (in order to prevent fraud)
- Log-in and passwords
- Product event logs eg. history of the end user's activity in AMC's services

-   Personal identity numbers and or other identity numbers (some banks require identity numbers when approving payments)

AMC might use biometric data for identification purposes in the AMC Application. If AMC make use of biometric data, AMC will collect clear permission directly from the data subject and provide the option not to use the function.

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

-   The Data Controller's end users
-   The Data Controller's staff
-   The Data Controllers customers and vendors

A.5. Processing has the following duration:

The processing of personal data is not time-limited and will be performed until the Agreements, or this DPA is terminated or cancelled by one of the Parties, unless mandatory Union or Member State law requires storage of the personal data.

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:

Name	VAT Number	Address	Processing Description
Microsoft Corporation	IE8256796U	South County Business Park, Carmanhall and Leopardstown, Dublin 18, Ireland	Cloud infrastructure provider
Sendinblue	FR80498019298	7 rue de Madrid, 75008 Paris, France	Email application service provider

The Data Controller shall on the commencement of the Clauses authorise the use of the abovementioned Sub-Processors for the processing described.

B.2. Prior notice for the authorisation of Sub-Processors

As AMC A/S continues to grow, the Sub-Processors that AMC A/S engage with may also change. AMC will inform the Data Controller in writing of any intended changes concerning the addition or replacement of Sub-Processors at least 1 months in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned Sub-Processor(s).

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:

- Processing personal data to be able to identify and communicate with the Data Controller's relevant personnel.
- Ensuring required personal data of end users and the staff are available to ensure sufficient security level of the services, including controlling who can give access to approve payments.
- Processing personal data relating to product event logs to be able to analyze recent activities in case of security breach.
- Processing IP-addresses to control geographical the use of our services, and to prevent potential cyber attacks.
- Processing personal data for fulfilling the obligations of delivering of the AMC services to the data controller.

C.2. Security of processing

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:

- That the Data Processor is, whenever possible and appropriate encrypt and pseudonymize personal data.
- The Data Processor shall, upon termination or expiration of the Agreements delete stored data, unless this contradicts with any existing law.
- Security measures as defined in the AMC Security Annex.

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:

- As defined in the AMC Security Annex.

Assistance to the Data Controller as defined in clause 9.1 and 9.2 will be executed as consultancy tasks and thereby billable unless the requested task is a minor task.

C.4. Storage period/erasure procedures

Personal data is stored for no longer than 5 years or until termination of the agreements after which the personal data is erased by the Data Processor unless Union or Member State law to which the Data Processor is subject requires longer retention.

Upon termination of the provision of personal data processing services, the Data Processor shall delete the personal data in accordance with Clause 11.1., unless the Data Controller – after the signature of the contract – has modified the Data Controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses. Additional costs arising in connection with special requests from the Data Controller about altering the Data Processor's storage/erasure procedures of personal data shall be borne by the Data Controller.

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:
- The Data Processor's premises and Sub-Processors' according to Appendix B.
- Microsoft Azure Data Center location in North Europe: Carmanhall and Leopardstown, Dublin, D18 P521, Írland.
- Microsoft Azure Data Center location in West Europe: Agriport 601, Middenmeer, Netherlands.

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

The Data Processor has obtained the Data Controller's approval to transfer personal data under the Clauses to third countries when using sub-processors.

Transfer of personal data to countries outside the EU/EEA is only approved by the Data Controller, if the Data Processor ensures a valid legal basis by entering into the EU Commission's standard contractual clauses (SCC) with additional supplementary measures to ensure compliance with the data protection legislation.

If the legal basis for transferring personal data requires the Data Controller to be a direct party therein, the Data Processor shall be considered authorized to enter into this on behalf of the Data Controller. This means that the Data Controller, where the SCC are used as basis for the transfer, shall be bound by the obligations imposed on the data exporter according to the SCC. The Data Processor can assign this authorization to the sub-processors so that these sub-processors can enter into a legal basis for transfer on behalf of the Data Controller.

In relation to the processing of personal data that requires the legal basis for transfer of personal data, the provisions in the SCC take precedence over the Clauses.

Thus, the Data Processor has the Data Controller's instruction to transfer personal data to third countries in accordance with the list of sub-processors, cf. Appendix B.

C.7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

To enable the Data Controller to exercise its responsibility to ensure the Data Processor is compliant with the GDPR, the Data Processor shall provide the Data Controller with an internal compliance report (Compliance Report). Such Compliance Report is provided upon request from the Data Controller, and the cost related to providing the report is to be invoiced to the Data Controller.

In the case the Data Controller does not find the Compliance Report sufficient to exercise its right to ensure processing is performed in accordance with law, the Data Processor shall, at the Data Controller's expense, obtain an inspection report from the Data Controller's representatives concerning the Data Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The Data Controller is entitled to audit those parts of the AMC services and processes that are used to provide services for The Data Controller. Date and time of the audit shall be notified beforehand to AMC, audit will be done during normal working hours. Such audit's will be supported by AMC consultancy and therefore be invoiced to the Data Controller according to the current list price.

The Data Controller is entitled to use a third party for the audit. The third party must agree on the same NDA as already agreed between the Data Controller and the Data Processor.

The Data Controller will hold AMC information made available during the audit confidential and use it only for monitoring the compliance with the actual agreement.

The report shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases, at own expense, request a new inspection under a revised scope and/or different methodology.

Based on the results of such an 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.

The Data Controller's costs, if applicable, relating to physical inspection shall be defrayed by the Data Controller. The Data Processor shall, however, be under obligation to set aside the resources (mainly time) required for the Data Controller to be able to perform the physical inspection. The Data Processors activities will be invoiced to the Data Controller according to list price.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by Sub-Processors

In case of clear instruction from the Data Controller, The Data Processor shall at the Data Controller's expense obtain an inspection report concerning the Sub-Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The activities will be invoiced to the Data Controller according to list price.

The inspection report shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases, at own expense, 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.