acubiz

Data Processing Agreement

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

with regard to the data processor's processing of personal data

The Customer
(hereinafter referred to as the "Data Controller")

&

Visma Acubiz A/S
VAT: 20 95 05 87
Gærtorvet 1-5
1799 København
Denmark
(hereinafter referred to as the "Data Processor")

(the data controller and the data processor hereinafter each referred to as a "party" and collectively as "the parties") HAVE AGREED, as an addendum to the parties' contract, on the following Contractual Clauses (hereinafter the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of privacy and fundamental rights and freedoms of individuals.

acubiz

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data processor when processing personal data on behalf of the data controller.

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 provision of the service Acubiz, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses supplements, and shall constitute an addendum to, the contract concluded between the parties regarding the data controller's access to the Acubiz EMS service (the said contract including any and all addendums thereto hereinafter referred to as "the Main Agreement"). The Clauses take precedence over any conflicting provisions in the Main Agreement. Likewise, the Clauses take precedence over corresponding provisions in other agreements between the parties which concern the data processor's processing of personal data in connection with providing the Acubiz EMS service under the Main Agreement. For the avoidance of doubt, it is noted that since the Clauses are an addendum to the Main Agreement, the framework provisions in the Main Agreement, including the regulation in the Main Agreement regarding breach of contract, liability (including in particular the exclusions and limitations of liability in the Main Agreement), choice of law and dispute resolution, also apply in relation to the Clauses, including in connection with a breach of the Clauses.

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 subjects 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 on certain other matters in relation to the Clauses.

10. The Clauses along with the appendices, as well as the Main Agreement and any other agreements which are of importance to or supplement these agreements, 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. Equally, the Clauses shall not exempt the data controller from obligations to which the data controller is subject pursuant to 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 things, for ensuring that the processing of personal data that the data processor is instructed to perform has a legal basis. Thus, in particular the data controller is responsible to the data processor for ensuring that:

a. The data controller has the necessary legal basis to process, and to entrust the data processor and its sub-processors to carry out the agreed processing of, the personal data which are processed in connection with performance of the Acubiz service;
b. The data controller's instructions, as expressed through these Clauses, the Main Agreement and any other agreements, are legal; and
c. The data controller does not transfer any other type of personal data to the data processor than what follows from the data controller's instruction, and that the transferred personal data do not relate to other categories of data subjects than the ones specified in the instruction.

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 processor is subject. Such instructions are specified in appendices A and C.

2. 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.

a. Except as otherwise specified below in Clause 4.2.b, however, the data processor may freely choose between accepting or rejecting any subsequent instruction; and the data processor is also entitled to make it a condition for acceptance of a subsequent instruction that the data controller pays a fee set by the data processor for carrying out the instruction, and/or that an increase, determined by the data processor, is made in the general remuneration that the data controller pays under the Main Agreement.
b. However, the data processor may not (unless it would be illegal for the data processor to carry out the instruction, see in that regard Clause 4.3. below) refuse to accept a subsequent instruction covered by no. i (meaning an instruction to provide a copy of the data controller's personal data) or ii (meaning an instruction to cease further processing of personal data) immediately below:
    i. An instruction to provide a copy of the data controller's personal data. However, the data processor is entitled to demand separate remuneration for carrying out such instruction. The remuneration is calculated on the basis of the time spent by the data processor to carry out the instruction and the data processor's generally applicable hourly rate for such work (if the Main Agreement sets out

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

specific hourly rates for work of the type in question, these hourly rates apply). In addition to this, the data processor is entitled to have any external expenses relating to carrying out the instruction, including expenses in relation to any necessary assistance from sub-processors, covered by the data controller. The details of how the copy shall be provided, including the format that the data is provided in, must be agreed upon between the parties in connection with the data controller's submission of the instruction.

ii. An instruction to cease further processing of personal data. If such an instruction is given, the data processor shall, notwithstanding that the Main Agreement has not yet been terminated in accordance with the Main Agreement's clauses of termination, act in accordance with Clause 11 ("Erasure of data") below. For the avoidance of doubt, it is noted that from the moment the instruction is complied with by the data processor, the data processor is released from its obligations to provide its services under the Main Agreement, since the Acubiz EMS service cannot be provided without processing of the personal data. Notwithstanding this, the data controller is still obliged to pay remuneration to the data processor pursuant to the Main Agreement in the period until the date when the Main Agreement would have expired if the data controller had, at the time of issuing the instruction, instead given a notice of termination for convenience in accordance with the Main Agreement's termination provisions (i.e., with the notice period required pursuant to the Main Agreement and subject to any provisions in the Main Agreement regarding when a notice of termination for convenience may at the earliest become effective). The remuneration for the period in question is calculated as the amount of remuneration that the data controller would have been obliged to pay for the services under the Main Agreement if the data controller had during the said period purchased the minimum amount of services that the data controller would have been obliged to pursuant to the Main Agreement.

3. 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

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 and – against separate remuneration to the data processor – all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR. Any separate remuneration to the data processor in accordance with the aforementioned is calculated on the basis of the time spent by the data processor in procuring the information, and the data processor's generally applicable hourly rates. Furthermore, the data processor is entitled to have any external expenses it may incur in procuring the information, including expenses in relation to any necessary assistance from sub-processors, covered by the data controller.

If – 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 of the GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

If the data controller, after having entered into the Clauses, argues that additional measures should be implemented other than those which are already, at the time of entering into the Clauses, specified in appendix C (or which the data processor otherwise may already have implemented), it is to be discussed between the parties whether an agreement on implementing such additional measures, including a timetable and remuneration to the data processor for such implementation (as well as a possible increase of the ongoing remuneration that the data controller pays for the services in accordance with the Main Agreement) can be reached. If the parties cannot come to an agreement, the data controller must, if the data controller cannot accept that processing of personal data takes place without implementation of the measures in question, instruct the data processor to cease further processing of the personal data. In such circumstances, Clause 4.2.b.ii above applies.

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 another processor (sub-processor) for the fulfilment of the Clauses without 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 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), see in this regard further Appendix B.2. A list of sub-processors which the data controller has at the time when the Clauses come into force authorised the use of can be found in Appendix B.1.

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. 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

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 of the 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.

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. process the personal data in a third country

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 of the GDPR on which they are based, shall be set out in Appendix C.6.

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

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 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 carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
c. 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;
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.

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 following from Clauses 9.1 and 9.2.

4. The data processor is entitled to separate remuneration for the assistance provided to comply with the data controller's requests under this Clause 9 ("Assistance to the data controller"). The remuneration is calculated on the basis of the time spent by the data processor and the data processor's generally applicable hourly rate for such work (if the Main Agreement sets out specific hourly rates for work of the type in question, these hourly rates apply), and in addition to this, the data processor is entitled to have any external expenses relating to complying with the request, including expenses in relation to any necessary assistance from sub-processors, covered by the data controller. However, with respect to assistance given in relation to the data controller's obligations under Articles 33-34 of the GDPR, the data processor is not entitled to remuneration for fulfilment of its obligations under Clause 10 ("Notification of personal data breach") below.

10. Notification of personal data breach

1. In case of any personal data breach at the data processor or a sub-processor regarding the personal data that the data controller has entrusted the data processor to process, the data processor shall without undue delay, after having become aware of the breach, notify the data controller of the personal data breach. The notification can be sent by e-mail to the contact address designated by the data controller. The notification can be submitted using a standard form.

2. 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) of the 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.

3. The data processor's notification to the data controller shall, if possible, be submitted in time so that the information as a whole is provided in such a way that the data controller can carry out the full notification to the supervisory authority within the time requirements for notifications regarding a personal data breach, which are specified in Article 33 of the GDPR.

4. If it is not possible for the data processor to provide the information as a whole, the information can be provided in phases without any undue further delay. In continuation of the initial notification to the data controller, the data processor shall therefore, if necessary, continuously update and complete the information to the data controller, such that the data controller, if necessary, can update a personal data breach notification to the supervisory authority, cf. Article 33(4) of the GDPR.

5. The data processor's notification of a personal data breach does not constitute an acknowledgement of fault or liability in regard to an occurred personal data breach.

6. 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 of data

1. On termination of the Main Agreement, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and confirm to the data controller that it has done so.

2. However, the data processor can still store the data controller's personal data after the termination of the Main Agreement if EU or Member State law requires the data processor to carry out such storage of the personal data. Under such circumstances, the data processor commits to exclusively process the personal data for the purposes and duration provided for by such law and under the conditions prescribed by the law.

3. If, after the Clauses were entered into, the data controller informs the data processor in writing that the data controller wants the data processor to return the personal data to the data controller on termination of the Main Agreement instead of just deleting them, the data processor shall accept such request for change of the Clauses (the change shall be documented and retained in writing, including electronically, by both parties in connection with the Clauses), and the data processor shall then on termination of the Main Agreement of course not delete its copies of the personal data pursuant to Clause 11.1 before the return of the personal data to the data controller has been carried out. In relation to the return of the data to the data controller, Clause 4.2.b.i will apply, including the terms therein on separate remuneration to the data processor.

12. Audit and inspection

1. The data processor shall, at the data controller's request, 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 on other clauses in relation to the Acubiz Service with regard to the personal data processing, 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 both parties' signature. If the parties have previously entered into a data processing agreement between them regarding the processing of personal data covered by the Clauses, the Clauses shall, from the date of both parties' signing of the Clauses, apply instead of such data processing agreement previously entered into.

2. Both parties shall be entitled to require the Clauses (including the appendices) renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation. If a change to the Clauses (including the appendixes) changes the data processor's obligations in such a way that it becomes more expensive for the data processor to comply with the Clauses, the data processor is, in connection with the changes of the Clauses, entitled to demand that the remuneration for the services under the Main Agreement be increased, and/or that additional terms regarding separate remuneration to the data processor is inserted in the Clauses, such that the data processor's increased expenses are covered.

3. The Clauses shall apply for the duration of the Main Agreement and until the data processor has deleted the data controller's personal data in accordance with the Clauses. In this period, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. Signatures

On behalf of the data controller:

Date	Name	Title	Signature

On behalf of the data processor:

Date	Name	Title	Signature
	Henrik Malling	Managing Director	

15. Data controller and data processor contacts/contact points

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

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

Contact details of the data controller:

Name	Title	Phone number	Email

Contact details for data processor:

Name	Title	Email
Vivi Sejrsen	Data Protection Manager	dpa.acubiz@visma.com
Rebecca Løssl	Legal & Compliance Specialist	dpa.acubiz@visma.com
Henrik Malling	Managing Director	dpa.acubiz@visma.com

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

The data processor's processing of the data controller's personal data is done with the agreed purpose of providing the Acubiz service and any related services as further described in the Main Agreement. The processing happens primarily in connection with the data controller's (including the data controller's configured Acubiz users) use of the Acubiz service.

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)

The data processor's processing of personal data for the data controller has the nature that follows from the Main Agreement, and among other things in particular include the following activities:

- Import and upload of the data controller's credit card transactions to Acubiz (NB: Acubiz is only responsible for the transport of the transactions) as well as storage of the data in the Acubiz solution.
- Making Acubiz, with the data stored therein, available for the data controller's users.
- Accessing the data in connection with error correction in the Acubiz EMS solution.
- Storage of data for archiving purposes.

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

The processing solely includes ordinary personal data (cf. Article 6 of the GDPR), including more specifically (depending on the data controller's specific configuration and use of the Acubiz EMS solution): name, initials, e-mail address, telephone number, address, employee number, company ID, configuration information (typically choice of language, username, password/passcode, approval limit, etc.), payment card details, bank details, and transaction data (typically information regarding amount, currency, date, country, type of cost, extract of credit card number and card holder identifier, account type, dimensions and possibly comments, as well as photo of payment document).

If the data controller has purchased the add-on service Mileage under the Main Agreement, the processing will also include ordinary personal data regarding driving, including (depending on the data controller's specific configuration and use of the Acubiz EMS solution) the purpose of the transportation, the license plate of the car (registration number), distance, the start and end address and, if location service has been chosen, GPS tracking data.

If the data controller has purchased the add-on service TIME under the Main Agreement, the processing will also include ordinary personal data regarding time registration. The composition of this data depends on the information demands specified by the data controller but can (depending on the data controller's specific configuration and use of the Acubiz EMS solution) e.g. be data on time spent with specification of account, type, dimensions and date.

<u>The Acubiz EMS solution is only intended for processing of ordinary personal data</u>
The data controller (including the data controller's configured users of the Acubiz EMS service)

must NOT enter or cause to be entered into the Acubiz EMS solution personal data which belongs to any of the following categories, as the solution is not intended for processing of personal data of such categories:

- Sensitive personal data (personal data covered by Article 9 of the GDPR), i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
- Personal data relating to criminal convictions and offences (personal data covered by Article 10 of the GPDR)
- Data regarding CPR numbers (or regarding any other national identification numbers/identifiers of general application for which specific conditions for processing apply pursuant to Member State law, cf. Article 87 of the GDPR).

The data processor disclaims any and all liability for processing of personal data of the mentioned categories that may happen as a consequence of the data controller's failure to adhere to the above.

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

Data is processed about the data controller's configured Acubiz EMS users. E.g., this may be the data controller's employees, board members, non-staff (volunteers) and teachers.

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

See Clauses 14.1 and 14.3.

Appendix B: Authorised sub-processors

Version June 2024

B.1. Approved sub-processors

On commencement (coming into force) of the Clauses, the data controller authorises the engagement of the following sub-processors:

Name	CVR / Reg. No.	Address	Location of processing	Description of processing
VISMA SOFTWARE INTERNATIONAL AS	NO-980 858 073	Karenslyst Allé 56, NO-0277 Oslo	NO - Within EØS	Hosting Center
Paperflow ApS	DK-37035785	Niels Juels Gade 5 DK-1059 København K	DK - Within the EU	Document scanning – Invoice Management Service

B.2. Intended changes concerning the addition or replacement of sub-processors.

The data processor has the data controller's general authorisation for the engagement of sub-processors.

The data processor shall inform the data controller in writing 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). If it is not immediately possible or is not possible without incurring disproportionate costs for the data processor to fulfil its delivery obligations under the Main Agreement during such notice period, the data processor shall be exempt from liability for this.

If the data controller objects to the addition or replacement of a sub-processor (see above), the data controller may, notwithstanding the ordinary notice period that pursuant to the Main Agreement applies to a termination for convenience, terminate the Main Agreement for convenience to expire just before the notified time where the use of the new sub-processor is to commence. If the data controller wishes to avail itself of this right of termination, a written notice thereof must be given to the data processor no later than 2 weeks after the time when the data processor sent the notification about the intended change. In the event that the data controller avails itself of the preceding right of termination, the data controller shall, irrespective of the

termination, still be obliged to continue to pay remuneration to the data processor pursuant to the terms of the Main Agreement during the period from the effective date of the termination and until the earliest date on which the Main Agreement would have expired if the data controller's notice of termination had instead been rendered pursuant to the terms in the Main Agreement itself (i.e., the Main Agreement excluding this data processing agreement) on termination for convenience (i.e., with the notice period required pursuant to the Main Agreement and subject to any provisions in the Main Agreement regarding when a notice of termination for convenience may at the earliest become effective). The remuneration for the period in question is calculated as the amount of remuneration that the data controller would have been obliged to pay for the services under the Main Agreement, based on the data controller's actual consumption for the previous three months, proportionally distributed per month throughout the notice period, but at least the agreed aconto/minimum consumption that the data controller would have been obliged to pursuant to the Main Agreement.

Except for the right to terminate the Main Agreement for convenience by notice of termination as set out above, the data controller's objection does not give rise to any rights for the data controller. Thus, if the data controller does not terminate the Main Agreement for convenience as set out above, the data controller must accept that the data processor at the notified time commences use of the new sub-processor in relation to the processing of the data controller's personal data.

Appendix C: Instruction pertaining to the use of personal data

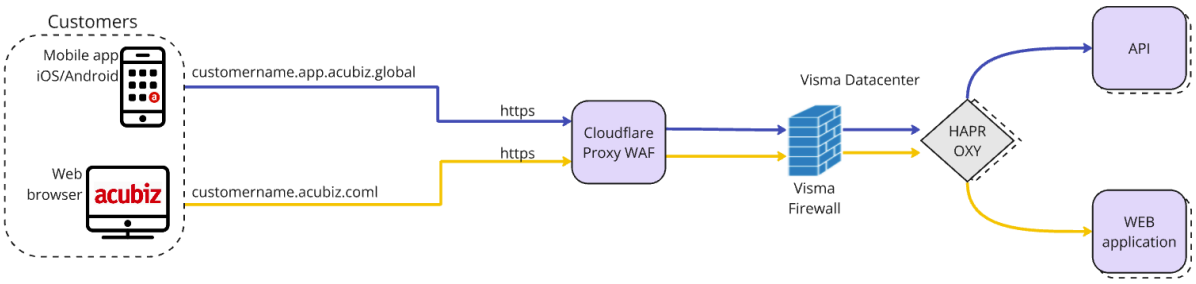
Version June 2024

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:

The data processor is instructed to process the data controller's personal data so that the Acubiz EMS service (including any add-on services purchased by the data controller under the Main Agreement) can be provided in accordance with the Main Agreement, with the agreed functionality therein, including especially by recording/importing, by storing and by making accessible (to the data controller with its users of the Acubiz service) for viewing, and performance of certain processing of, the personal data that the data controller (including via the data controller's configured users of the service) loads or allows to be loaded into the Acubiz service (among other things import of transaction data from the credit card company(ies) used by the data controller).

The figure below illustrates import and upload of the data controller's credit card transactions to Acubiz. (NB: Acubiz is only responsible for the transport of the transactions)



C.2. Security of processing

The level of security shall take into account the following: Considering, among other things, (i) that the processing only includes ordinary personal data (cf. Article 6 of the GDPR), (ii) that the data is furthermore limited to relatively few types of data, and (iii) that the data – in light of the purpose of the Acubiz EMS solution – concerns transactions made by the data controller's users in a commercial context, the risk relating to rights and freedoms of individuals is low. The data processer's level of security shall reflect this risk assessment (and the data controller thus accepts that the data processor shall not be required to establish a higher level of security than one that reflects this risk assessment).

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:

- Acubiz is a SaaS provider. Our office and our production are separated, i.e. we can only access the customer's data at the Visma datacenter through Visma security measures such as Zscaler, Firewalls, DMZ, etc., and we do not have physical access to the customer's data.
- All customer data is stored at the Visma datacenter in Norway. Customer data is not stored anywhere else, neither on employees' PCs nor in other cloud solutions.
- All data is encrypted at the Visma datacenter (encryption at rest).
- All operation are conducted without the use of the individual employee's hard disk drive.
- No PCs are left in the office when we go home - everything is mobile - and all employees must authenticate via Visma's Zscaler to access the servers at the Visma datacenter.
- All employees at Acubiz have signed non-disclosure agreements.
- Acubiz utilises the following security technologies: Cloudflare proxy, web application firewall, Visma firewall, NAT & haproxy, network segmentation (VLAN), DMZ, and Zscaler (comparable to a very advanced VPN solution).
- The servers in the Visma datacenter are hardend, and ongoing security updates are conducted for all servers.
- The Visma datacenter performs general IT security LOG monitoring of firewalls and servers, which are actively monitored 24/7/365. Acubiz has entered into an agreement with the Visma datacenter for incident handling and remediation, and the Visma datacenter uses the latest technologies to scan for security risks.
- Acubiz and Visma continuously conduct penetration tests to monitor and optimise the security of the customer's data.
- Acubiz has entered into an agreement with the Visma datacenter to ensure high availability/uptime for the Acubiz Service.
- Acubiz performs a back-up of all customer solutions in Acubiz once a day.

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:

Re Clause 9.1:

The data processor shall, at the request of the data controller, assist the data controller to the necessary extent with retrieval of specific data that is processed on behalf of the data controller. The data processor shall ensure that the data processor's systems and internal processes are, to a reasonable extent, designed in such a way that it is possible for the data processor to provide assistance to the data controller in cases where the data controller is not able to retrieve the specific data without the data processor's assistance.

Re Clause 9.2:

The data processor shall assist the data controller with necessary information in accordance with Clause 10. The data processor's systems and internal processes shall be designed in a way that facilitates this to a reasonable extent.

C.4. Storage period/erasure procedures

While the Main Agreement is in force, data (incl. personal data) must, as a starting point, cf. further below, be stored for at least 5 + 1 years:

Storage:

- Current calendar year appendix
- At least the 5 preceding calendar years' annexes
- The above is part of the regular subscription under the Main Agreement

Deletion:

- All attachments that are older than the above-mentioned 5+1 years, the data processor is entitled – but not obliged – to delete.
- This does not apply, however, if a written agreement has been reached in the Main Agreement (e.g. via an addendum thereto) regarding the data controller's purchase of long-term archive storage, in which case the data processor is first entitled to delete in accordance with the thus agreed longer archive retention period.
- Deletion can also take place in accordance with specific written instructions that the data controller may give to the data processor. Such an instruction - with a specific indication of the data that is to be deleted - can be submitted using a form which can be requested from the data processor. For carrying out deletion in accordance with specific instructions, the data processor is entitled to charge a separate remuneration, which is calculated on the basis of the time consumption the data processor uses for the deletion, as well as the data processor's general applicable time rates.

Upon termination of the Main Agreement, the data processor must delete the personal data in accordance with Provision 11.1. For the sake of clarity, it should be noted that if it is agreed in the Main Agreement (typically in the form of an addendum to the Main Agreement regarding the purchase of a special archive solution) that the data must continue to be stored by the data processor in an archive solution for a period after the termination of the services of the Main Agreement, deletion from such a special archive solution in accordance with Provision 11.1 will of course only take place at the time of the end of the archive solution (as the Main Agreement in such a situation, regardless of whether it may otherwise have ended, precisely as far as the archive solution is concerned remains in force until termination of the special archive solution).

C.5. Processing location

The data processor's processing of the personal data covered by the Clauses takes place, in the case of the data processor itself, on one or more addresses located in the EU/EEA, and, in the case of sub-processors, within the locations (areas) which are specified in appendix B.1 or which – if it is a new sub-processor appointed according to Appendix B.2 – may have been specified by the data processor in connection with the notification regarding the data processor's intention to start using the new sub-processor. If the data controller wants more precise information regarding the addresses applicable at any given time for the processing of personal data, the data controller may contact the data processor.

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

Third countries (non EU Member States)

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.

Since the data controller has not in these Clauses provided a documented instruction regarding transfer of personal data to a third country, it follows from the above that the data processor is not, at the time when these Clauses are entered into, entitled to perform such transfers within the framework of the Clauses.

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

Auditor's report

If the data processor annually has an ISAE 3402 II auditor's report (or other equivalent auditor's report, e.g. an ISAE 3000 I auditor's report) prepared by a third party concerning matters relating to compliance with the GDPR, the data controller can download a copy of the auditor's report free of charge on the data processor's website here:

https://acubiz.com/legal/auditors-reports/

The data controller understands that any such auditor's report will be a report of a general nature, which thus does not deal with customer-specific matters (and thus does not deal with matters that may be specific to the processing of personal data that the data processor performs for the data controller).

Audit

The data controller has a right to carry out, when it deems it necessary, an audit of the data processor's processing of personal data on behalf of the data controller.

The data controller may choose to carry out an audit either as a written inspection or by way of a physical inspection.

The audit can be performed by the data controller itself or in collaboration with a third party. The data processor is entitled to object to a third party which has been designated by the data controller to carry out the inspection, if the designated person/organization, in the data processor's reasonable assessment, is not suitable or qualified to carry out the inspection, including because the person/organization (i) is not independent, (ii) is, or is affiliated with or has relations to, a direct competitor to the data processor, or (iii) is otherwise obviously unfit to perform the task. If the data processor makes such an objection to the designated person/organization, the data controller must appoint another person/organization to carry out the audit.

An inspection must be based/focused on the security measures agreed between the parties (see Appendix C.2), the data processor's fulfilment of the instructions, including the use of sub-processors, and compliance with any requirements for assistance to the data controller.

In regard to a physical inspection, the data controller must give at least ten (10) days prior notice. The data controller and/or the data controller's representative participating in the inspection must also submit to the data processor's general security measures and agree to a confidentiality clause on normal terms directly with the data processor. The data controller or its representative may then have access to carry out physical inspection of the places where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for or in connection with the processing.

Costs and remuneration

The data controller's possible expenses in connection with performance of an audit, including any physical inspection, are borne by the data controller itself. The data processor is entitled to remuneration in connection with the data controller's exercise of an audit. The remuneration is calculated on the basis of the data processor's time spent and the data processor's hourly rates applicable at the relevant time, with the addition of any positive costs incurred, including costs incurred by the data processor in connection with any assistance from sub-processors.

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

The data processor shall, at its own expense, carry out appropriate supervision regarding the sub-processors' compliance with the GDPR, other applicable EU law or Member State data protection provisions and these Clauses, in relation to the processing activities performed by such sub-processors for the data processor.

Thus, supervision (audit/inspection) of the sub-processors used by the data processor takes place through the data processor, and the data processor determines on its own the specific procedure (including whether the supervision may be carried out via obtaining auditor's reports) and frequency. At the request of the data controller, the data processor shall provide documentation of the supervision (including a copy of any relevant auditor's reports that the data processor may have received via the sub-processor).

Notwithstanding the above, the data controller may – if justified and reasonably necessary – when the sub-processor allows this, choose to initiate and/or participate in a written inspection or on a physical inspection at the sub-processor. This may become relevant if the data controller reasonably considers that the data processor's supervision of the sub-processor has not provided the data controller with sufficient assurance that the sub-processor's processing is in accordance with the GDPR, other applicable EU law or Member State data protection provisions and these Clauses. Any inspection of a sub-processor must take place in compliance with the sub-processor's conditions for inspection. When the data controller initiates and/or participates in an inspection in relation to a sub-processor, the rules in Appendix C.7 above shall apply correspondingly.

Costs and remuneration

Any expenses incurred by the data controller in connection with performance of an audit/inspection, including any physical inspection, of a sub-processor that the data controller has initiated and/or participated in are borne by the data controller itself. The data processor is entitled to remuneration in connection with the data controller's exercise of such audit/inspection, including any physical inspection, that the data controller has initiated and/or participated in. The remuneration is calculated on the basis of the time spent and the data processor's and sub-processor's hourly rates applicable at the relevant time, with the addition of any positive costs incurred, including costs incurred by the data processor in connection with any assistance from sub-processors.

Appendix D: The parties' terms of agreement on other matters