

Data Processing Agreement

Standard Contractual Clauses

in accordance with Article 28(3) of Regulation (EU) 2016/679 (General Data Protection Regulation) regarding the data processor's processing of personal data

between

Visma IMS
Søren Frichs Vej 44D
8230 Åbyhøj

CVR-nr 25862015

hereafter "the data controller"

and

Heysender ApS
Jens Baggesens Vej 47
8200 Aarhus N, Denmark
CVR. No. 31282322

hereafter "the data processor"

each of which is a "party" and together constitute "the parties"

HAS AGREED to the following standard contractual clauses (the Provisions) to comply with the General Data Protection Regulation and ensure the protection of privacy and the fundamental rights and freedoms of natural persons.

1. Content

2. Preamble 3

3. The Rights and Obligations of the Data Controller..... 3

4. The Data Processor Acts According to Instructions 4

5. Confidentiality..... 4

6. Security of Processing 4

7. Use of Sub-Processors 5

8. Transfer to Third Countries or International Organizations 6

9. Assisting the Data Controller..... 6

10. Notification of a Personal Data Breach 7

11. Erasure and Return of Information 7

12. Audits, Including Inspection 7

13. The Parties' Agreement on Other Matters 8

14. Commencement and Termination..... 8

15. Contact Persons of the Data Controller and Data Processor..... 8

Appendix A Information About the Processing 10

Appendix B Sub-Processors 11

Appendix C Instruction Relating to the Processing of Personal Data..... 12

Appendix D The Regulation of Other Matters..... 15

2. Preamble

1. These Provisions determine the data processor's rights and obligations when he/she processes personal data on behalf of the data controller.
2. These Provisions have been designed to ensure the parties' compliance with Article 28(3) in Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC (the General Data Protection Regulation).
3. In connection with the provision of the Heysender solution, the data processor processes personal data on behalf of the data controller in accordance with these Provisions.
4. The Provisions take precedence over any corresponding provisions in other agreements between the parties.
5. These Provisions come with four appendixes, and the appendixes form an integral part of the Provisions.
6. Appendix A contains detailed information about the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects, and the 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 which the data controller has approved.
8. Appendix C contains the data controller's instructions regarding the data processor's processing of personal data, a description of the security measures that the data processor as a minimum must implement, and how the data processor and any sub-processors are audited.
9. Appendix D contains provisions regarding other activities not covered by the Provisions.
10. The Provisions and appendixes must be kept in writing, including electronically, by both parties.
11. These Provisions do not release the data processor from obligations imposed on the data processor under the General Data Protection Regulation or any 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 happens in accordance with the General Data Protection Regulation (see Article 24 of the Regulation), data protection regulations under other Union or Member State¹ law, and these Provisions.
2. The data controller has the right and duty to make decisions in terms of for which purpose(s) and with which means personal data may be processed.
3. The data controller is responsible for, among other things, ensuring that there is a basis for processing personal data, which the data processor is instructed to carry out.

¹ References to "Member State" in these provisions should be understood as a reference to "the EEA Member States."

4. The Data Processor Acts According to Instructions

1. The data processor must only process personal data upon documented instructions from the data controller, unless required by Union or Member State law to which the data processor is subject. These instructions must be specified in Appendix A and C. Subsequent instructions can also be given by the data controller while personal data is being processed, but the instructions must always be documented and stored in writing, including electronically, along with these Provisions.
2. The data processor immediately informs the data controller if an instruction, in his/her opinion, violates this regulation or the data protection regulations under other Union or Member State law.

5. Confidentiality

1. The data processor may only grant access to personal data which is processed on behalf of the data controller to persons who are subject to the data processor's instructions, who are committed to confidentiality, or who are subject to an appropriate statutory obligation of confidentiality, and only to the extent necessary. The list of persons who have been granted access must be continuously reviewed. On the basis of this review, access to personal data can be denied if access is no longer necessary and the personal data must then no longer be available to these persons.
2. Upon request from the data controller, the data processor must be able to demonstrate that the persons in question, who are subject to the data processor's instructions, are subject to the above-mentioned obligation of confidentiality.

6. Security of Processing

1. Article 32 of the General Data Protection Regulation states that the data controller and data processor, taking into account the current technical level, the implementation costs, and the nature, scope, context, and purpose of the processing in question as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, carry out the appropriate technical and organizational measures to ensure a level of protection appropriate to these risks.

The data controller must assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to address these risks. Depending on their relevance, they may include:

- a. pseudonymization and the encryption of personal data
 - b. the ability to ensure ongoing confidentiality, integrity, availability, and resilience of the processing systems and services
 - c. the ability to promptly restore the availability of and access to personal data in case of a physical or technical incident
 - d. a procedure for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures to ensure the security of the processing.
2. According to Article 32 of the Regulation, the data processor must—independently of the data controller—also assess the risks the processing poses to the rights of natural persons and implement measures to address these risks. With this evaluation in mind, the data controller must make the necessary information available to the data processor, which enables him/her to identify and assess such risks.

3. In addition, the data processor must assist the data controller to ensure his/her compliance with the data controller's obligation in accordance with Article 32 of the Regulation by, among other things, making the necessary information available to the data controller regarding the technical and organizational security measures, which the data processor has already implemented in accordance with Article 32 of the Regulation, and all other information that is necessary for the data controller to comply with his/her obligation in accordance with Article 32 of the Regulation.

If addressing the identified risks—in the data controller's assessment—requires the implementation of additional measures to the measures that the data processor has already implemented, the data controller must indicate the further measures to be implemented in Appendix C.

7. Use of Sub-Processors

1. The data processor must meet the conditions referred to in Article 28(2) and (4) of the General Data Protection Regulation to make use of another data processor (a sub-processor).
2. The data processor must thus not use a sub-processor to fulfill these Provisions without prior general written approval from the data controller.
3. The data processor has the data controller's general approval for use of sub-processors. The data processor must notify the data controller in writing of any planned changes regarding the addition or replacement of sub-processors with at least 30 days' notice and thereby give the data controller the opportunity to object to such changes before the use of the said sub-processor(s). A longer notice period in connection with specific processing activities can be specified in Appendix B. The list of sub-processors that the data controller has already approved is in Appendix B.
4. When the data processor makes use of a sub-processor in connection with the execution of specific processing activities on behalf of the data controller, the data processor must, via a contract or another legal document in accordance with Union or Member State law, impose on the sub-processor the same data protection obligations as those set out in these Provisions, whereby the necessary guarantees are made to ensure that the sub-processor will complete the technical and organizational measures in such a way that the processing complies with the requirements of these Provisions and the General Data Protection Regulation.

The data processor is therefore responsible for demanding that the sub-processor as a minimum complies with the data processor's obligations under these Provisions and the General Data Protection Regulation.

5. Sub-processor agreement(s) and any subsequent changes thereto are sent—at the request of the data controller—in copy to the data controller, who thereby is able to ensure that similar data protection obligations as a result of these Provisions are imposed on the sub-processor. Provisions on commercial terms that do not affect the legal content of the sub-processor agreement regarding data protection should not be sent to the data controller.
6. The data processor must include the data controller in its agreement with the sub-processor as a beneficiary third party in the event of the data processor's bankruptcy, so the data controller can assume the rights of the data processor and assert them against sub-processors, which, e.g., enables the data controller to instruct the sub-processor to delete or return the personal data.
7. If the sub-processor does not fulfill its data protection obligations, the data processor remains fully responsible to the data controller for the fulfillment of the sub-processor obligations. This does not affect the rights of the data subjects, which follow the General Data Protection Regulation, including in particular Articles 79 and 82 of the Regulation, against the data controller and the data processor, including the sub-processor.

8. Transfer to Third Countries or International Organizations

1. Any transfer of personal data to third countries or international organizations must only be done by the data processor on the basis of documented instructions to this effect from the data controller and must always be done in accordance with Chapter V of the General Data Protection Regulation.
2. If the transfer of personal data to third countries or international organizations, which the data processor has not been instructed to carry out by the data controller, is required under Union or Member State law to which the data processor is subject, the data processor must notify the data controller about this legal requirement before processing, unless the law in question prohibits such notification for reasons of vital public interests.
3. As such, without documented instructions from the data controller, the data processor cannot, within the framework of these Provisions:
 - a. transfer personal data to a data controller or data processor in a third country or an international organization
 - b. leave the processing of personal data to a sub-processor in a third country
 - c. process the personal data in a third country
4. The instructions of the data controller regarding the transfer of personal data to a third country, including the basis for the transfer as in Chapter V of the General Data Protection Regulation, must be stated in Appendix C.6.
5. These Provisions must not be confused with the Standard Contractual Clauses as referred to in Article 46(2), points (c) and (d), and these Provisions cannot constitute a basis for the transfer of personal data as referred to in Chapter V of the General Data Protection Regulation.

9. Assisting the Data Controller

1. The data processor assists to the extent possible, taking into account the nature of the processing, the data controller by means of appropriate technical and organizational measures with the fulfillment of the data controller's obligations to respond to requests about the exercise of the data subjects' rights as stipulated in Chapter III of the General Data Protection Regulation.

This entails that the data processor, to the extent possible, must assist the data controller in connection with the data controller ensuring compliance with:

- a. the duty to provide personal data when such is collected from the data subject
 - b. the duty to provide personal data if the personal data has not been collected from the data subject
 - c. the right of access
 - d. the right to rectification
 - e. the right to erasure ("the right to be forgotten")
 - f. the right to restriction of processing
 - g. the 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 automatic processing, including profiling
2. In addition to the data processor's obligation to assist the data controller in accordance with Provision 6.3., the data processor also, taking into account the nature of the processing and the information available to the data processor, assists the data controller with:
 - a. the data controller's obligation to report a personal data breach to the competent supervisory authority, the Danish Data Protection Agency, without undue delay and if possible no later than 72 hours after he/she has become aware of it, unless it is unlikely that the personal data breach entails a risk to the rights and freedoms of natural persons

- b. the data controller's obligation to notify the data subject without undue delay of a personal data breach when the breach is likely to entail a high risk for the rights and freedoms of natural persons
 - c. the data controller's obligation to carry out an analysis, prior to the processing, of the consequences of the intended processing activities for the protection of personal data (an impact assessment)
 - d. the data controller's obligation to consult the competent supervisory authority, the Danish Data Protection Agency, before processing, if an impact assessment regarding data protection shows that the processing will lead to high risk in the absence of measures taken by the data controller to limit the risk.
3. The parties must indicate in Appendix C the necessary technical and organizational measures with which the data processor must assist the data controller and to what extent and scale. This applies to the obligations arising from Provisions 9.1. and 9.2.

10. Notification of a Personal Data Breach

1. The data processor notifies the data controller without undue delay upon becoming aware of the personal data breach.
2. The data processor's notification to the data controller must, if possible, be given no later than 24 hours after the data processor has become aware of the breach, so the data controller can comply with his/her obligation to report the personal data breach to the competent supervisory authority, cf. Article 33 of the General Data Protection Regulation.
3. In accordance with Provision 9.2.a., the data processor must assist the data controller in reporting the breach to the competent supervisory authority. This means that the data processor must assist in providing below information, which according to Article 33(3) must be present in the data controller's report of the breach to the competent supervisory authority:
 - a. the nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects as well as the categories and the approximate number of personal data records affected
 - b. the likely consequences of the personal data breach
 - c. the measures that the data controller has taken or suggests taken to address the personal data breach, including, if relevant, measures to mitigate its possible adverse effects.
4. The parties must indicate in Appendix C the information that the data processor must provide in connection with his/her assistance to the data controller in his/her obligation to report the personal data breach to the competent supervisory authority.

11. Erasure and Return of Information

1. Upon termination of the services relating to the processing of personal data, the data processor is required to delete all personal data that has been processed on behalf of the data controller and confirm to the data controller that the data has been deleted, unless Union or Member State law prescribes the storage of the personal data.

12. Audits, Including Inspection

1. The data processor provides the data controller with all the data that is necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and these Provisions, and enables and contributes to the audits, including inspections, carried out by the data controller or another auditor, who is authorized by the data controller.
2. The procedures for the data controller's audits, including inspections, with the data processor and sub-processors are detailed in Appendix C.7. and C.8.

3. The data processor is obligated to give supervisory authorities who by law have access to the facilities of the data controller or data processor, or representatives who act on behalf of the supervisory authorities, access to the physical facilities of the data processor against legitimate identification.

13. The Parties' Agreement on Other Matters

1. The parties can agree on other provisions with regard to the service concerning the processing of personal data, e.g. liability, as long as these provisions not only directly or indirectly violate the Provisions or impair the data subject's fundamental rights and freedoms as stipulated in the General Data Protection Regulation.

14. Commencement and Termination

1. The Provisions enter into force on the date of both parties' signature hereof.
2. Both parties can require the Provisions renegotiated if changes to the law or inadequacies in the Provisions give rise to this.
3. The Provisions are effective as long as the service concerning the processing of personal data lasts. During this period, the Provisions cannot be terminated unless other provisions managing the provision of the service relating to the processing of personal data are agreed upon by the parties.
4. If the provision of the services relating to the processing of personal data ceases and the personal data is deleted or returned to the data controller in accordance with Provision 11.1. and Appendix C.4., the Provisions may be terminated by both parties giving written notice.
5. Signature

On behalf of the data controller

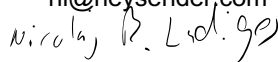
Name Dan Thordahl Jørgensen
 Telephone number
 E-mail dan.jorgensen@visma.com
 Titel Managing Director

Signature

On behalf of the data processor

Name Nicolaj Balle Ladiges
 Title Managing director
 Telephone number 26 85 34 14
 E-mail nl@heysender.com

Signature



15. Contact Persons of the Data Controller and Data Processor

1. The parties can contact each other via the below contact persons.
2. The parties are obligated to inform each other of changes relating to the contact persons.

Name Maria Høj Radmer
 Telephone number 24499972
 E-mail mhr@ims.dk
 Titel Produktchef

Name Søren Skou Jessen
Telephone number 29365154
E-mail soren.jessen@visma.com
Titel Legal Counsel

Name Niels Mørk
Telephone number 42 54 56 57
E-mail gdpa@heysender.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

Receipt of e-mail address, the content of e-mails as well as any merge fields with data belonging to the data subject (hereafter the recipient). Data is received and stored with the purpose of delivering e-mails to the recipient.

A.2. The data processor’s processing of personal data on behalf of the data controller primarily concerns (the nature of the processing)

- The development and support of the Heysender system, which is an ESP/SMTP solution to send e-mails and transactional e-mails.
- The data processor provides the data controller with the Heysender system. The data controller’s e-mails and e-mail addresses are stored here.
- The Heysender system sends, on behalf of the data controller, newsletters/e-mails to the data controller’s recipients—and provides support.
- The provision of support and consulting services.

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

The type of data that is processed is data that is typically sent by e-mails.

For example

- The contact’s first name and surname
- The contact’s e-mail address and phone number
- The contact’s interests and preferences
- Gender
- Date of birth
- Address
- Postcode, city, and country

The data controller is able to send further information, including any sensitive personal data, via e-mail to the data subject. The data processor must be informed and notified in advance by the data controller if the data controller wants Heysender to process sensitive personal data.

A.4. The processing includes the following categories of the data subject

Includes all the persons (with addresses and merge-field data) to whom the data controller wants to send e-mails, including, among other things, the data controller’s customers and employees.

Stores data about the data controller’s employees, provided they have access to the platform.

A.5. The data processor’s processing of personal data on behalf of the data controller can begin after these Provisions enter into force. The processing has the following duration

The processing of personal data is not time-limited and lasts until the collaboration agreement ends.

The data processor may keep a backup of the data controller’s data to the extent necessary. The data processor must not keep a backup for a period longer than 12 months after the end of the main agreement.

Appendix B Sub-Processors

B.1. Approved sub-processors

Upon the Provisions' commencement, the data controller has approved the use of the following sub-processors

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Team.Blue Denmark A/S	29412006	Højvangen 4, 8660 Skanderborg	Data hosting
Ubivox Technologies ApS	27379494	Østre Stationsvej 43, 3., 5000 Odense C	E-mail services
Heyloyalty	29394458	Jens Baggesens Vej 47. 8200 Aarhus N	Administration and operation

Upon the commencement of the Provisions, the data controller has approved the use of the above sub-processors for the described processing activities. The data processor must not—without the written approval of the data controller—use a sub-processor for a processing activity other than the one described and agreed upon or use another sub-processor for this processing activity.

B.2. Notice for approval of sub-processors

The data processor is obliged to announce additions or changes to the list of sub-processors with 30 days' notice. If the data controller can argue why he/she cannot accept a new sub-processor or changes to existing sub-processors, the data controller may terminate the main agreement at the end of a subscription period.

C.1. The subject matter of and instructions for the processing

The data processor's processing of personal data on behalf of the data controller is accomplished by the data processor performing the following:

The data processing is performed for the fulfillment of the collaboration agreement between the parties as well as the provision of the services the data controller has purchased from Heysender and which are stipulated on the data controller's Heysender account, cf. further on this in section A.2.: the nature of the processing.

C.2. Security of processing

The level of security must reflect:

- The data processor performs the necessary technical and organizational measures to ensure data protection in accordance with the data protection legislation and in accordance with Article 32 as well as Article 25 of GDPR about data protection by design and by default.
- The data processor has mapped out his/her processing of personal data, including an assessment of the sensitivity. In addition, the data processor has carried out a security assessment of all data locations, including all data transfer points, and implemented security measures relevant in relation to the risk assessment for the classified personal data.
- The data processor's technical and organizational security measures thus prevent personal data from being accidentally or illegally destroyed, lost, or degraded, whilst also preventing it from becoming known to unauthorized persons, being misused, or otherwise being illegally processed.

General security measures

- The data processor must implement encryption and pseudonymization of personal data as risk-reducing factors where the data processor deems it relevant.
- The data processor must limit access to personal data to the relevant persons to comply with the requirements and obligations of the collaboration agreement.
- The data processor must implement systems that can detect, restore, address, and report incidents in relation to personal data.
- The data processor must ensure that the transfer of personal data to sub-processors is done responsibly.
- The data processor has ensured that all access to personal data from the data controller or his/her representatives is done via SSL encryption.
- The software provided in the collaboration agreement includes a user management system that enables the data controller to manage the data controller's representatives' access to personal data.
- The data processor has established a hosting platform that ensures that all personal data is responsibly saved and that data cannot be accessed unintentionally, as well as associated backup systems that ensure that all data can be restored in the event of incidents on the hosting platform.
- The data processor has implemented software and procedures to continuously ensure that internal IT security is at a high level.

Authorization and access control

All access to personal data happens via authorization with a personal username and password in the internal systems, which the data processor has established to comply with his/her obligations in relation to the collaboration agreement and the data processing agreement. The data processor has ensured that the sub-processors use authorization and access control to the Heysender system, in connection with their services (if there is a need for the sub-processors' access).

External communication links

All access to the Heysender system is via SSL encryption. When sending e-mails, the email is TLS encrypted if the contact's e-mail client accepts this. Forced TLS is an option when sending.

Control of denied access attempts

Unintentional access is prevented by firewalls so repeated attempts to access servers are blocked.

Logging

- A log is kept of the date and representative of the data processor when personal data is accessed as part of the fulfillment of the collaboration agreement

Home and/or remote workplaces

- The data processor's processing of personal data can be done using home and/or remote workplaces.
- Access to personal data is via encrypted traffic (HTTPS) to and from Heysender, using industry-standard SSL certificates.
- All employees of the data processor that are authorized to process the data are subject to a confidentiality agreement and have received the relevant training in personal data security and are only allowed to use personal data as part of the fulfillment of the data processor's obligations and rights in relation to the collaboration agreement with the data controller.

C.3. Assisting the data controller

The data processor must to the extent possible—within the below scope and extent—assist the data controller in accordance with Provisions 9.1. and 9.2. by completing the following technical and organizational measures:

The data processor assists the data controller in ensuring his/her compliance with the obligations in Articles 32–36 of the Regulation in relation to, among other things, security measures, reporting security breaches, and any consulting with the supervisory authorities.

The data processor provides all necessary information so the data controller can document that the processing by the data processor meets the obligations and allows and contributes to the control and audits thereof. Hereunder, the data processor is obliged to inform the data controller if it is the data processor's belief that an instruction is illegal.

The data processor thus informs the data controller that the collection of personal data must occur in accordance with the applicable legislation. Specifically, the data controller is notified that contacts must give informed, definite consent to the intended data use if consent is necessary according to the applicable legislation. The data processor also informs the data controller that the sending of e-mails using Heysender is done in plain text, which is a medium unsuitable to contain sensitive personal data, and that the receiver's access to their own personal data should be password-protected. Unencrypted e-mails are also considered an unsuitable medium for general personal data, such as name and address.

C.4. Storage period/erasure routine

The personal data is stored by the data processor as long as the collaboration lasts or until the data controller requests the data to be deleted or returned.

The data processor must, at the request of the data controller, delete or return all personal data to the data controller, or a third party appointed by the data controller, as well as delete all copies, unless legislation requires a copy of the personal data stored. If the data processor

does not receive other instructions from the data controller or the appointed third party, the personal data is deleted 120 days from the end of the collaboration.

If the data controller instructs the return or handover of personal data, the data controller determines at the time of the return how and to which storage medium the personal data should be returned. The medium chosen must be customary for such data transfers.

C.5. Location of processing

The processing of the personal data covered by the Provisions cannot be done at any other locations than the following without the data controller's prior written approval:

- Heysender's office in Aarhus or one of the employee's addresses due to remote working.
- The addresses of the approved sub-processors (stated in Appendix B.1.).
- The personal data the data processor receives from the customer's contacts are stored with a third party. The data are stored on servers in Denmark that are owned by the company Team.Blue Denmark A/S with whom a data processing agreement has been entered into such that the data security is guaranteed.
- If the customer wants to use a third party that is not integrated directly with Heysender, this responsibility will fall on the customer.

C.6. Instructions regarding the transfer of personal data to third countries

If the data controller does not in these Provisions or afterward give documented instructions regarding the transfer of personal data to a third country, the data processor is not allowed to make such transfers within the framework of these Provisions, unless such transfer takes place to one of the authorized sub-processors mentioned in Appendix B. The basis for transfer is used in accordance with Chapter V of the General Data Protection Regulation on transfers of personal data to third countries or international organisations. The specific transfer basis shall follow from the applicable Annex B.

C.7. The procedures for the data controller's audits, including inspections, of the processing of personal data entrusted to the data processor

The data controller can audit the data processor when, according to the data controller's assessment, a need for this arises.

At appropriate intervals and with proper notice, the data controller or a representative of the data controller has the right to carry out physical inspections of the data controller concerning the compliance with the data processing agreement. The data controller's inspection can furthermore be carried out by means of questionnaires, requests for the provision of documentation, statements, etc.

Any costs of the data controller as part of the inspection are borne by the data controller alone. The data processor, however, is obliged to allocate the resources (primarily the time) necessary for the data controller to complete his/her inspection.

The data processor's time, beyond the first 4 hours, can be settled according to the data processor's regular hourly rates and according to the time spent. In this case, this must be agreed upon prior to the individual inspection.

If the data processor wants another type of inspection, e.g. an ISAE 3000 auditor statement from an independent third party in relation to the data processor's compliance with the General Data Protection Regulation, the data processor offers the preparation of such at the data controller's own expense.

C.8. The procedures for audits, including inspections, of the processing of personal data entrusted to sub-processors

It is the responsibility of the data processor to audit any sub-processors in an appropriate manner in relation to the sub-processors' compliance with the General Data Protection Regulation, data protection provisions under other Union or Member State law, and these Provisions. The data processor is entitled to assess for himself/herself what constitutes an appropriate inspection, taking into account the specific risk associated with the processing by the sub-processor.

In addition to the planned inspection, an inspection of the sub-processor can be carried out when, according to the data processor (or the data controller), a need for this arises.

Documentation of the data processor's inspection of the sub-processor is sent to the data controller without undue delay. The data controller can contest the framework and/or method of the inspection and can in such cases request the completion of a new inspection within a different framework and/or using a different method.

Based on the results of the inspection, the data controller is entitled to request the implementation of further measures to ensure compliance with the General Data Protection Regulation, data protection provisions under other Union or Member State law, and these Provisions.

Appendix D The Regulation of Other Matters by the Parties

Section 7.6.

The data processor informs that no agreement can be entered into with sub-processors in the event of bankruptcy. The data processor is instructed to delete data in the event of non-payment, and the data processor keeps a local copy of the backup, which can be used to restore the data in collaboration with the liquidator.

In the event of the customer's bankruptcy, a "Bankruptcy account" is created. All personal data will be deactivated but not deleted from the database. The account will exist until the bankruptcy is settled or until further has been agreed with the liquidator.



Section 11.1.

The data processor informs that data is stored in a backup for up to 12 months from the end of services. The data protection agreement is enforced as long as data is stored.

April 2023

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet med Addo Sign sikker digital underskrift. Underskrivers identitet er fysisk registreret i det elektroniske PDF dokument og vist herunder.

Underskrivere



Dan Thordahl Jørgensen
Adm. direktør
de2b3991-8331-4eb8-a569-e048555495f4 07-08-2023 17:07

Dokumenter i transaktionen

Heysender-VISMA Data Processing Agreement (DPA)_English_19.04.2023.pdf

Nærværende dokument



Dokumentet er underskrevet digitalt med Addo Sign sikker signeringservice. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument.

Dokumentet er låst for ændringer og tidsstempelt med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i PDF dokumentet, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan verificeres dokumentets ægthed

Dokumentet er beskyttet med Adobe CDS certifikat. Når dokumentet åbnes i Adobe Reader, vil det fremstå som være underskrevet med Addo Sign signeringservice.