Data Processing Agreement

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

between

Visma Local Government A/S
CBR.no. 37 09 89 22
Søren Frichs Vej 44D
8230 Åbyhøj
Denmark

(the data processor)

And

team.blue Denmark A/S
CBR.no: 29 41 20 06
Højvangen 4
8660 Skanderborg
Denmark

(the sub-processor)

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.

Version 2.0

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data processor and the sub-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 provision of Services as set out in the Hosting agreement, the sub-processor will process personal data on behalf of the data processor in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties as well as replace any previous data processing agreement(s) agreed 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 processor's conditions for the sub-processor's use of additional sub-processors and a list of sub-processors authorised by the data processor.

8. Appendix C contains the data processor's instructions with regards to the processing of personal data and the minimum-security measures to be implemented by the sub-processor.

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 sub-processor from obligations to which the sub-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 and sub-processor is instructed to perform, has a legal basis.

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

4. The sub-processor acts according to instructions

1. The sub-processor shall process personal data only on documented instructions from the data processor, unless required to do so by Union or Member State law to which the sub-processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data processor 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 sub-processor shall immediately inform the data processor if instructions given by the data processor, in the opinion of the sub-processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The sub-processor shall only grant access to the personal data being processed on behalf of the data processor to persons under the sub-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.

2. The sub-processor shall at the request of the data processor demonstrate that the concerned persons under the sub-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 processor and sub-processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data processor 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 sub-processor shall also – independently from the data processor – 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 processor shall provide the sub-processor with all information necessary to identify and evaluate such risks.

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

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

   If the data processer requires stricter safety measures in relation to what is already agreed between the parties pursuant to the Clauses and Appendix C, the sub-processor will, to the extent it is possible, implement such measures, provided that the sub-processor receives payment, therefore.

7. Use of sub-processors

1. The sub-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 will consent to the sub-processor's use of additional sub-processors, provided that the provisions set out in the Clauses are complied with. The data processor can check at any time to see the sub-processor's additional sub-processors by visiting the sub-processor's website at www.dandomain.dk/compliance. Any changes to the additional sub-processors will be reported to the data processor by e-mail.

3. Where the sub-processor engages an additional sub-processor for carrying out specific processing activities on behalf of the sub-processor, the same data protection obligations as set out in the Clauses shall be imposed on that additional 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 sub-processor shall therefore be responsible for requiring that the additional sub-processor at least complies with the obligations to which the sub-processor is subject pursuant to the Clauses and the GDPR.

4. If the data processor wishes to give direct instruction to the additional sub-processors, they should not do so until it has been discussed with and via the sub-processor. If the data processor gives direct instructions to the sub-processors, then the data processor must inform the sub-processor of such instructions and relevant background information either beforehand or at the time the instructions are given. When the data processor gives direct instructions to the additional sub-processors, a) the sub-processor will be exempt from all responsibilities and any consequences of such instructions will be the sole responsibility of the data processor, b) the data processor will be responsible for covering all costs that the instructions may cause the sub-processor to incur and the sub-processor will also have the right to charge the data processor its standard hourly rate for time spent on all work that such instructions would entail for the sub-processor and c) the data processor is responsible for any costs, fees or other payments for the sub-processors incurred by such direct instructions.

5. By entering into the Clauses, the data processor acknowledges that the sub-processor is entitled to add and replace additional sub-processors, provided that a) any new sub-processors comply with the corresponding provisions set out in this Clause 7 for current sub-processors and that b) the data processor is notified by email about any new sub-processors by no later than 14 days before the date on which the new sub-processor begins processing personal information that are released by the data processor to the sub-processor.

6. If the data processor does not wish for the sub-processor to use a new sub-processor about which the data processor was notified, cf. Clause 7.5, then the data processor must lodge an objection against the use of the new sub-processor in writing to the sub-processor no later than 7 days after the data processor received the notification about the new sub-processor. If the sub-processor is unable to accommodate the data processor's objection against a new sub-processor, it must notify the data processor as soon as possible. In such case, the data processor can then terminate the main agreement with one month's notice starting on the first day of the month. The objection must be objectively justified before it can result in such a notice of cancellation.

7. The list of sub-processors already authorised by the data processor can be found in Appendix B.

8. If the additional sub-processor does not fulfil their data protection obligations, the sub-processor shall remain fully liable to the data processor as regards the fulfilment of the obligations of the additional 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. Returning and/or deletion of personal data in the event of the data processor's bankruptcy

1. In order to accommodate the data processor's data controller/end customer in the event of the liquidation of the data processor, the following section has been implemented in the Clauses. The validity of the provisions assume that an agreement has been entered into between the data processor and the data controller/end customer approving that, in the event of the bankruptcy of the data processor, the data controller/end customer shall have the right to have data returned or deleted at the sub-processor.

2. If the data processor is subject to bankruptcy proceedings, liquidation proceedings or similar, upon request from the data controller/end customer, the sub-processor shall return or delete data which the data controller/end customer owns. The sub-processor may only execute the return or deletion of data in accordance with this provision.

3. The sub-processor shall only be able to return or delete the data controller's/end customer's data if:

   - The data processor has ensured the isolation of the data controller's/end customer's services in such a way so that the sub-processor is able to identify the data controller/end customer's data.
   - The data controller/end customer can provide documentation that it is the owner of the relevant data.
   - The data controller/end customer may, if possible, prompt the data processor's bankruptcy estate to make the necessary resources available to the sub-processor, including in the form of employees for the purpose of making it possible for the data controller/end customer to retrieve or delete their own data. Similarly, the data controller/end customer shall also make the necessary resources available for this. Any costs connected to the bankruptcy estate or the data controller's/end customer's use of resources, is not the concern of the sub-processor.

4. To the best of their ability, the sub-processor shall assist in finding the data controller's/end customer's data and shall, to the extent possible, assist in meeting the data controller's/end customer's requirements for the returning or deletion of the relevant data. In all instances, the sub-processor shall be entitled to demand payment for time spent for the work the sub-processor performs in pursuance of this agreement. If not already agreed, the fee shall be calculated according to the sub-processor's, at any time, applicable hourly rates. The data controller/end customer shall be liable for such payment to the sub-processor if payment for the fee cannot be achieved from the data processor's company or from the bankruptcy estate. The sub-data processor and the party submitting the request for the return of the personal data must agree on the amount of remuneration before the work is performed.

5. If the data controller/end customer has given the sub-processor instructions to return or delete data and, even though the sub-processor has taken the necessary initiatives to ensure that the instruction was warranted, proves to be unwarranted, the liability lies solely with the data controller/end customer which shall, consequently, be liable for compensation for any loss the sub-processor may suffer as a result.

9. Transfer of data to third countries or international organisations

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

2. In case transfers to third countries or international organisations, which the sub-processor has not been instructed to perform by the data processor, is required under EU or Member State law to which the sub-processor is subject, the sub-processor shall inform the data processor 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 processor, the sub-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 an additional sub-processor in a third country

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

4. The data processor'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.

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

10. Assistance to the data processor

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

   This entails that the sub-processor shall, insofar as this is possible, assist the data processor in the data processor'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 sub-processor's obligation to assist the data processor pursuant to Clause 6.3., the sub-processor shall furthermore, taking into account the nature of the processing and the information available to the sub-processor, assist the data processor in ensuring compliance with:

   a. The data processor's obligation to assist the data controller 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 processor's obligation to assist the data controller 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 processor's obligation to assist the data controller 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 processor's obligation to assist the data controller 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 processor to mitigate the risk.

3. The data processor is responsible for covering all costs incurred by the sub-processor in connection with such assistance, cf. Clause 10, including the cost of additional sub-processors. The price for the sub-processor's assistance will be calculated according to the currently applicable hourly rate for the performance of such work.

11. Notification of personal data breach

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

2. The sub-processor's notification to the data processor shall, if possible, take place without undue delay after the sub-processor has become aware of the personal data breach to enable the data processor to notify the data controller enabling the data controller to comply with the obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 10(2)(a), the sub-processor shall assist the data processor in notifying the personal data breach to the data controller, meaning that the sub-processor is required to assist in obtaining the information listed below which, pursuant to Article 33 (3) GDPR, shall be stated in the data processor's notification to the data controller:

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

12. Erasure and return of data

1. On termination of the provision of personal data processing services, the sub-processor shall be obligated to return all the personal data to the data processor and delete any existing copies on the request of the data processor and confirm that it has done so unless Union or Member State law requires storage of the personal data.

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

13. Audit and inspection

1. The sub-processor shall make available to the data processor 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 processor or another auditor mandated by the data processor.

2. Procedures applicable to the data processor's audits, including inspections, of the sub-processor and additional sub-processors are specified in the following clauses.

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

4. If the data processor wishes to have another or additional audit reports drawn up or affect the timing of any reports, in addition to the audit reports that the sub-processer already draws up on its own initiative, or wants an inspection of the processing of personal data carried out by the sub-processor or additional sub-processor, then this is further agreed with the sub-processor.

5. When an audit is carried out at the request of the data processor, from third parties at the request of the data processor, or from authorities due to conditions of the data processor, the data processor will cover all costs in connection with inspecting the security conditions of the sub-processor, as well as those of additional sub-processors. The sub-processor will also be entitled to charge the data processor its standard hourly rate for time spent on all work that such an inspection would entail for the sub-processor.

14. 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.

15. Commencement and termination

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

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

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 processor pursuant to Clause 12.1, the Clauses may be terminated by written notice by either party.

5. Signature

On behalf of the data processor

Name	Kasper Lyhr
Position	CEO
Date	29-06-2021
Signature	Kasper

On behalf of the sub-processor

Name Stefan Rosenlund
Position Managing Director
Date 06 / 30 / 2021
Signature

16. Data processor and sub-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.

The data processor

Name Søren Skou Jessen
Position Compliance Consultant
E-mail Dataprivacy@firstagenda.com

Name Josefine Høgh Pedersen
Position Compliance and legal manager
E-mail compliance@curanet.dk

Appendix A - Information about the processing

A.1. The purpose and the nature of the sub-processor’s processing of personal data on behalf of the data processor is:

The Sub-processor will during the term of this Agreement and as a part of the Services provided, process personal data on behalf of the Data Processor for the purpose of storing the personal data in question.

The Sub-processor agrees not to process personal data for any other purposes and only in accordance with this Agreement.

A.2. The processing includes the following types of personal data about data subjects:

All personal data submitted by the data processor on behalf the data controllers. This means all categories of personal data can be processed by the sub processor.

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

The users, customers and/or employees of the data controllers and data processor.

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

The sub-processor shall process personal data on behalf of the Data Processor for the duration of the Agreement unless otherwise instructed by the Data Processor.

Appendix B Authorised additional sub-processors

B.1. Approved sub-processors

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

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
PING IT A/S	34471967	Vandmanden 24, DK, 9200 Aalborg, Danmark	Erasure of data and decommissioning of hardware
B4Restore	27719945	Aahave Parkvej 31, 8260 Viby J, Danmark	Outsourced services for IBM Spectrum (TSM) backup services.

Appendix C - Instruction pertaining to the use of personal data

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

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

The Sub-processor will during the term of this Agreement and as a part of the Services provided, process personal data on behalf of the Data Processor for the purpose of storing the personal data in question.

C.2. Security of processing

The level of security shall take into account:

Introduction

As a hosting provider, our most important security task is to take good care of your data and make sure that we always meet the security requirements of our customers.
Therefore, security is an area that we take very seriously - at all levels.

Organization of security

We have established an industry-leading information security programme (ISMS) that gives our customers the best protection and highest degree of confidence.
The program follows the ISO 27001 security standard, which we have been certified for since 2015.

Policies, procedures and standards

We have defined a set of policies, procedures and standards for how we operate in the company and take the best care of your data. The documents are regularly updated in line with the changing of our risk assessment. In this way we ensure that we always prioritize our efforts where they are needed the most.

Employee security

All employees and consultants with access to systems and facilities are subject to our security policies. Everyone undergoes security awareness training where they are presented with all relevant and current privacy and security topics. This occurs both upon commencement and continuously throughout their employment. The purpose is to equip employees so they can cope with actual threats against company and customer data.
In order to boost the overall level in the industry and to maintain own competences, our employees participate actively in communities and exchange of experience groups. We encourage our employees to constantly stay abreast of the latest developments and to acquire the highest certifications within security, networks, etc.

Dedicated security and personal data competences

Our security manager is responsible for implementing and maintaining our information security programme. Our internal auditor regularly reviews our security setup and reports directly to management. Finally, we have internal, legal competences within personal data, ensuring that personal data is processed according to the applicable rules both within the company and on behalf of our customers.

Operational security - Protection of customer data

The main task in our security programme is to take good care of your data. To do this, our security environment is divided into several layers:

- Physical security
  Our data centres are state-of-the-art and located in Denmark. Therefore, you can be sure that your data remains within the country. Our data centre provider is responsible for the physical environment such as power, cooling, fire fighting and access control, and we carry out stringent checks that our subcontractors always comply with the applicable security regulations for this field.

- Network
  Our network is segmented, so customers are protected from each other and from threats that move across the network. Firewalls restrict attacks on customers' environments, and DDoS protection limits the impact a potential attack might have on the servers. Advanced network inspection detects patterns and attack attempts from known malicious IP addresses and alerts our operations department if necessary.

- Logical access
  We only assign rights to employees who need them and we evaluate them regularly. Only specially privileged employees have access to manage the internal systems.

- Monitoring
  We monitor our infrastructure and relevant services around the clock. All deviations are registered in our incident management system. In addition to monitoring, we have assigned a 24/7 on-call service.

- Logging
  We log all access to management and customer environments. In this way, we ensure integrity and traceability and can combine incidents. Our central log platform ensures that we can quickly correlate logs from many sources.

- Backup
  We perform backup based on the agreed SLA. Backup data is always mirrored between two physically independent locations, so a copy is always available in case of a critical failure.

Business continuity and disaster recovery

Business continuity is about being prepared for incidents that may have a critical or disastrous impact on operations. Therefore, we have contingency plans which determine our procedures, routines and roles in the event of a disaster. Employees are trained for such an emergency several times a year.

To secure our technical infrastructure and to spread the risk of critical failure, we use multiple independent data centre providers. We always keep at least one copy of the backup data in a data centre where we do not have production data.

Audit, compliance and independent third-party assessments
We have a comprehensive compliance programme to ensure that we comply with agreed standards, internal policies and relevant legislation in the field, the purpose of which is to support and safeguard your business:

- ISO 27001
  ISO 27001 is an international standard for information security management. Several of our competitors claim that they follow the standard, but are not certified. We have been certified since March 2015. The certification must be renewed every year and is audited by both internal and external auditors.

- ISAE 3402 Type 2
  ISAE 3402 Type 2 describes how we secure the services we provide to our customers, and contains an independent auditor's conclusion on whether the description of our controls are accurate, appropriately designed, and whether the controls have functioned effectively throughout the audited period.

- Penetration testing
  We conduct regular penetration tests on critical components in our infrastructure to see how our systems defend themselves against external threats. Customers can also perform penetration tests on their own systems following prior arrangement with us.

Changes to security measures
The Sub-processor is always entitled to implement alternative security measures, provided that such security measures as a minimum are equivalent to or provide greater security than the security measures described in Appendix C. The Sub-processor cannot reduce the level of security without the Data Processor's prior written authorisation.

The above-mentioned reports and certifications are those that are currently being obtained to review team.blue Denmark's security measures. The Sub-processor are at all times entitled to obtain other types of reports or certifications to review and control relevant security measures ie. ISAE 3000, SOC2.

C.3. Assistance to the Data Processor

The Sub-processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data processor in accordance with Clause 10.1. and 10.2. by implementing the following technical and organisational measures:

For all services, customers themselves can answer and fulfil requests from data subjects to comply with the data subject's rights.

The Sub-processor must assist the Data processor as far as possible with fulfilling the Data processor's obligations to respond to registered data subjects to exercise their rights if the Sub-processor is the one that processes such personal information.
The Sub-processor will promptly inform the Data processor when the Sub-processor receives such enquiries from data subjects.
The Data processor is responsible for covering all costs incurred by the Sub-processor in connection with such assistance, cf. Clause 10.1 and 10.2, including the cost of additional sub-processors. The price for the Sub-

processor’s assistance will be calculated according to the currently applicable hourly rate for the performance of such work.

C.4. Storage period/erasure procedures

The Sub-processor is bound by the Clauses for as long as the Sub-processor processes personal data on behalf of the Data processor, given that the Data processor informs the Sub-processor in writing as soon as possible and within 14 days of the termination of the Data Processing Agreement of whether the Sub-processor should return or delete the processed personal data. 30 days after the termination of the Data Processing Agreement, the Sub-processor is entitled to delete all personal data that was processed on behalf of the Data processor. The Sub-processor must always store the processed data if it is provided for by EU law or the national law of the Member States.

C.5. Processing location

Personal data is processed at the locations listed below and at the additional sub-processor’s operational addresses.

Locations of the Sub-processor:

Headquaters: Højvangen 4, 8660, Skanderborg;
Datacenter #1: 8660 Skanderborg, Denmark;
Datacenter #2: 8660 Skanderborg, Denmark;
Datacenter #3: 8270 Højbjerg, Denmark;
Datacenter #4: 8362 Hørning, Denmark

The exact addresses of our data centers are kept confidential for security reasons. The Data processor can always find the addresses (postal code and city) of the data centers and the headquarters of the ISO 27001 certificate issued to team.blue Denmark A/S.

If the Data processor has obtained approval to carry out a physical audit of the facilities, the audit begins at the Sub-processor's headquarters, after which any external auditors will be escorted to the relevant data center.

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

The Sub-processor shall not transfer personal data to third countries. If such transfers become necessary to provide the Services, the Sub-processor and the Data Processor shall enter into EU Model Clauses.

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

C.7. Procedures for the Data processor’s audits, including inspections, of the processing of personal data being performed by the Sub-processor

If the Data processor wishes to conduct an inspection as stated in this sec C.7, the Data processor must always notify the Sub-processor at least 30 days ahead of time.

The Sub-processor will annually obtain a generally acknowledged and independent third party to submit an audit report devised in accordance with an accepted audit standard that describes and reviews the Sub processor's security measures. The Data Processor is entitled to receive a copy thereof. A copy of such audit report can always be obtained by the Data Processor on the Sub-processor's website.

If the Sub-processor wishes to have another or additional audit reports drawn up or affect the timing of any reports, in addition to the audit reports that the Sub-processor already draws up on its own initiative, or wants an inspection of the processing of personal data carried out by the Sub-processor or additional sub-processor, then this is further agreed with the Sub-processor.

When an audit is carried out at the request of the Data processor, from third parties at the request of the Data processor, or from authorities due to conditions of the Data processor, the Data processor will cover all costs in connection with inspecting the security conditions of the Sub-processor. The
Sub-processor will also be entitled to charge the Data processor its standard hourly rate for time spent on all work that such an inspection would entail for the Sub-processor.

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

To ensure that we operate as efficiently as possible, we use sub-processors for selected services. If there is a possibility that those sub-processors may have an impact on our security environment, we ensure that they comply with the same stringent requirements as ourselves through contracts, data processing agreements, auditor statements, self-regulation and non-disclosure agreements. We regularly check that our sub-processors comply with the requirements.

When an audit is carried out at the request of the Data processor, from third parties at the request of the Data processor, or from authorities due to conditions of the Data processor, the Data processor will cover all costs in connection with inspecting the security conditions of the additional sub-processors. The Sub-processor will also be entitled to charge the Data processor its standard hourly rate for time spent on all work that such an inspection would entail for the Sub-Processor. The Data processor will also be responsible for paying the additional sub-processors for time spent on all work that such an inspection would entail for the sub-processors.

Appendix D – The parties' terms of agreement on other subjects

HELLOSIGN

Audit trail

TITLE	DRAFT Visma - Data Processing Agreement (sub)
FILE NAME	DRAFT Visma - Dat...reement (sub).pdf
DOCUMENT ID	95f9ef25135c5f5fac5507ad84e9d2c11c604772
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Completed

Document history

SENT	**06 / 30 / 2021** 08:18:47 UTC	Sent for signature to Stefan Rosenlund (stefan.rosenlund@team.blue) from christine.fogt@team.blue IP: 185.25.142.131
VIEWED	**06 / 30 / 2021** 08:19:42 UTC	Viewed by Stefan Rosenlund (stefan.rosenlund@team.blue) IP: 87.104.85.252
SIGNED	**06 / 30 / 2021** 08:20:00 UTC	Signed by Stefan Rosenlund (stefan.rosenlund@team.blue) IP: 87.104.85.252
COMPLETED	**06 / 30 / 2021** 08:20:00 UTC	The document has been completed.