

## Data Processing Agreement

by and between

<b>Data Controller:</b>	xxx
Organisation number:	xxx
Country of establishment:  (or if established outside the EU, the EU country where the data controller makes use of the services from Visma)	
Data Controller's contact for general requests regarding the agreement (name, role, contact details):	
Data Controller's contact for notification of unauthorised data processing (name, role, contact details):	
<b>Data Processor:</b>	Visma Software AS
Organisation number:	933646920
Country of establishment:	Norge
Data Processor's contact for general requests regarding the agreement (name, role, contact details):	Visma Software AS Kundesenteret@visma.com Tlf. 09101 (08-17)
Data Processor's contact for notification of unauthorised data processing (name, role, contact details):	Visma Software AS Kundesenteret@visma.com Tlf. 09101 (08-17)

Henceforth respectively referred to as "Controller", "Processor", or "Party" and collectively as the "Parties".

### Introduction

Both Parties confirm that the undersigned have the power of attorney to enter into this data processing agreement ("Agreement"). This Agreement will form part of and regulate the processing of personal data tied to the following service agreements ("Service Agreements") between the Parties:

- *Avtale om bruksrett og leie av Huldt & Lillevik Lønn 5.0 Cloud*

The Processor operates in accordance with the Visma group Privacy Statement, available at <https://www.visma.com/privacy-statement/>, which is applicable to all companies within the Visma group.

## **Definitions**

The definition of Personal Data, Special Categories of Personal Data (Sensitive Personal Data), Processing of Personal Data, Data Subject, Controller and Processor is equivalent to how the terms are used and interpreted in applicable privacy legislation, including the General Data Protection Regulation (GDPR) applicable for this Agreement and Europe from 25 May 2018.

## **Scope**

The Agreement regulates the Processor's Processing of Personal Data on behalf of the Controller, and outlines how the Processor shall contribute to ensure privacy on behalf of the Controller and its registered Data Subjects, through technical and organisational measures according to applicable privacy legislation, including the GDPR.

The purpose behind the Processor's Processing of Personal Data on behalf of the Controller is to fulfill the Service Agreements and this Agreement.

This Agreement takes precedence over any conflicting provisions regarding the Processing of Personal Data in the Service Agreements or in other agreements made between the Parties. This Agreement is valid for as long as the Parties have a valid Service Agreement which includes Processing of Personal Data.

## **The Processor's obligations**

The Processor shall only Process Personal Data on behalf of and in accordance with the Controller's instructions. By entering into this Agreement, the Controller instructs the Processor to process Personal Data in the following manner; i) only in accordance with applicable law, ii) to fulfill all obligations according to the Service Agreement, iii) as further specified via the Controller's ordinary use of the Processor's services and iv) as specified in this Agreement.

The Processor has no reason to believe that legislation applicable to it prevents the Processor from fulfilling the instructions mentioned above. The Processor shall, upon becoming aware of it, notify the Controller of instructions or other Processing activities by the Controller which in the opinion of the Processor, infringes applicable privacy legislation.

The categories of Data Subject's and Personal Data subject to Processing according to this Agreement are outlined in Appendix A.

The Processor shall ensure the confidentiality, integrity and availability of Personal Data according to privacy legislation applicable to the Processor. The Processor shall implement systematic, organisational and technical measures to ensure an appropriate level of security, taking into account the state of the art and cost of implementation in relation to the risk represented by the Processing, and the nature of the Personal Data to be protected.

The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible and taking into account the nature of the Processing and the information available to the Processor, in fulfilling the Controller's obligations under applicable privacy legislation with

regards to request from Data Subjects, and general privacy compliance under the GDPR article 32 to 36.

If the Controller requires information or assistance regarding security measures, documentation or other forms of information regarding how the Processor processes Personal Data, and such requests exceed the standard information provided by the Processor to comply with applicable privacy legislation as Processor, and imposes additional work on the Processor, the Processor may charge the Controller for such additional services.

The Processor and its staff shall ensure confidentiality concerning the Personal Data subject to Processing in accordance with the Agreement. This provision also applies after the termination of the Agreement.

The Processor will, by notifying the Controller without undue delay, enable the Controller to comply with the legal requirements regarding notification to data authorities or Data Subjects about incidents.

Further, the Processor will to the extent it is appropriate and lawful notify the Controller of;

- i) requests for the disclosure of Personal Data received from a Data Subject,
- ii) requests for the disclosure of Personal Data by governmental authorities, such as the police

The Processor will not respond directly to requests from Data Subjects unless authorised by the Controller to do so. The Processor will not disclose information tied to this Agreement to governmental authorities such as the police, hereunder Personal Data, except as obligated by law, such as through a court order or similar warrant.

The Processor does not control if and how the Controller uses third party integrations through the Processor's API or similar, and thus the Processor has no ownership to risk in this regard. The Controller is solely responsible for third party integrations.

### **The Controller's obligations**

The Controller confirms by the signing of this Agreement that:

- The Controller shall, when using the services provided by the Processor under the Services Agreements, process Personal Data in accordance with the requirements of applicable privacy legislation.
- The Controller has legal authority to process and disclose to the Processor (including any subcontractors used by the Processor) the Personal Data in question.
- The Controller has the sole responsibility for the accuracy, integrity, content, reliability and lawfulness of the Personal Data disclosed to the Processor.
- The Controller has fulfilled all mandatory requirements and duties to file notifications with or get authorisation from the relevant regulatory authorities regarding the processing of the Personal Data.
- The Controller has fulfilled its duties to provide relevant information to Data Subjects regarding processing of Personal Data according to mandatory data protection legislation.
- The Controller agrees to that the Processor has provided guarantees with regards to implementation of technical and organisational security measures sufficient to safeguard Data Subject's privacy rights and their Personal Data.
- The Controller shall, when using the services provided by the Processor under the Services Agreement, not communicate any Sensitive Personal Data to the Processor, unless this is explicitly agreed in Appendix A to this Agreement.
- The Controller shall maintain an up to date register over the types and categories of Personal data it Processes, to the extent such Processing deviates from categories and types of Personal Data included in Appendix A.

### **Use of subcontractors and transfer of data**

As part of the delivery of services to the Controller according to the Service Agreements and this Agreement, the Processor may make use of subcontractors. Such subcontractors can be other

companies within the Visma group or external third party subcontractors located within or outside the EU. The Processor shall ensure that subcontractors agree to undertake responsibilities corresponding to the obligations set out in this Agreement. All use of subcontractors is subject to the Visma group Privacy Statement.

The Controller may request to include an overview of the current subcontractors with access to Personal Data in an Appendix B, and in any case, such an overview may be given on Visma's dedicated web pages for privacy compliance. The Controller may also request a complete overview and more detailed information about such subcontractors involved in the Service Agreements at any time.

If the subcontractors are located outside the EU, the Controller gives the Processor authorisation to ensure proper legal grounds for the transfer of Personal Data out of the EU on behalf of the Controller, hereunder by entering into EU Model Clauses or transferring Personal Data in accordance with the Privacy Shield.

The Controller shall be notified in advance of any changes of subcontractors that Process Personal Data. If the new subcontractor is demonstrably non-compliant with applicable privacy legislation, then the Controller may terminate this Agreement. Such termination may give the right to terminate the Service Agreement, partly or fully, according to the termination clauses included in the Service Agreement. An important part of such assessments shall be to what extent the subcontractor's Processing of Personal Data is a necessary part of the services provided under the Service Agreement. The change of subcontractor will not in itself be considered as a breach of the Service Agreement.

By signing this Agreement, the Controller accepts the Processor's use of subcontractors as described above.

## **Security**

The Processor is committed to provide a high level of security in its products and services. The Processor provides its security level through organisational, technical and physical security measures, according to the requirements on information security measures outlined in GDPR article 32.

Further, the internal privacy framework developed by the Visma group aims to safeguard the confidentiality, integrity, resilience and availability of Personal Data. The following measures are of particular importance in this regard:

- Classification of Personal Data to ensure implementation of security measures equivalent to risk assessments.
- Assess use of encryption and pseudonymization as risk mitigating factors.
- Limiting access to Personal Data to those that need access to fulfill obligations according to this Agreement or the Service Agreement.
- Manage systems that detects, restore, prevents and reports privacy incidents.
- Use security self assessments to analyze whether current technical and organisational measures are sufficient to protect Personal Data, taking into account the requirements outlined in applicable privacy legislation.

## **Audit rights**

The Controller may audit the Processor's compliance with this Agreement up to once a year. If required by legislation applicable to the Controller, the Controller may request audits more frequently. To request an audit, the Controller must submit a detailed audit plan at least four weeks in advance of the proposed audit date to the Processor, describing the proposed scope, duration, and start date of the audit. If any third party is to conduct the audit, it must as a main rule be mutually agreed between the Parties. However, if the processing environment is a multitenant environment or similar, the Controller gives the Processor authority to decide, due to security reasons, that audits shall be

performed by a neutral third party auditor of the Processor's choosing.

If the requested audit scope is addressed in an ISAE, ISO or similar assurance report performed by a qualified third party auditor within the prior twelve months, and the Processor confirms that there are no known material changes in the measures audited, the Controller agrees to accept those findings instead of requesting a new audit of the measures covered by the report.

In any case, audits must be conducted during regular business hours at the applicable facility, subject to the Processors policies, and may not unreasonably interfere with the Processors business activities.

The Controller shall be responsible for any costs arising from the Controller's requested audits. Assistance from the Processor that exceed the standard service provided by the Processor and/or Visma group to comply with applicable privacy legislation, will be subject to fees.

### **Term and termination**

This Agreement is valid for as long as the Processor processes Personal Data on behalf of the Controller according to the Service Agreements.

This Agreement is automatically terminated upon termination of the Service Agreement. Upon termination of this Agreement, the Processor will delete or return Personal Data processed on behalf of the Controller, according to the applicable clauses in the Service Agreement. Unless otherwise agreed in writing, the cost of such actions shall be based on; i) hourly rates for the time spent by the Processor and ii) the complexity of the requested process.

The Processor may retain Personal Data after termination of the Agreement, to the extent it is required by law, subject to the same type of technical and organisational security measures as outlined in this Agreement.

### **Changes and amendments**

Changes to the Agreement shall be included in a new Appendix to this Agreement and signed by both Parties in order to be valid.

If any provisions in this Agreement become void, this shall not affect the remaining provisions. The Parties shall replace the void provision with a lawful provision that reflects the purpose of the void provision.

### **Liability**

For the avoidance of doubt the Parties agree and acknowledge that each Party shall be liable for and held accountable to pay any and all administrative fines which a Party has been imposed to pay in accordance with GDPR. The liability for any and all other violations of the provisions of this Agreement or obligations under GDPR shall be governed by the liability clauses in the Service Agreements between the Parties. This also applies to any violation committed by the Processor's subcontractors.

### **Governing law and legal venue**

This Agreement is subject to the governing law and legal venue as set out in the Service Agreement between the parties.

\*\*\*\*

This Agreement has been drawn up in two (2) copies, of which the parties retain one copy each.

**Data Controller:**

Signature:

Signed by:

Place and date:

**Data Processor:**

Signature:

A handwritten signature in black ink that reads "Erlend Sogn". The signature is written in a cursive style with a large, prominent loop at the end of the word "Sogn".

Signed by:

CEO, Erlend Sogn

Place and date:

07.05.2018 Oslo

**Appendix A - Categories of Personal Data and Data Subjects**

*1. Categories of Data Subject's and Personal Data subject to Processing according to this Agreement*

- a. Categories of Data Subjects
  - i. customer end users
  - ii. customer employees
  - iii. customer contact persons
  - iv. ETC
  
- b. Categories of Personal Data
  - i. contact information such as name, phone, address,email etc.
  - ii. job information such as position, company etc
  - iii. economical information such as salary, credit card etc

*2. Types of sensitive Personal Data subject to Processing according to the Agreement*

This section is only relevant if the Processor shall process sensitive Personal Data as indicated below on behalf of the Controller as part of the Services Agreement. In order for the Processor to process such data on behalf of the Controller, the types of Sensitive Personal Data in question must be specified below by the Controller.

The Controller is also responsible for informing the Processor of, and specifying below, any additional types of sensitive Personal Data according to applicable privacy legislation.

The Processor shall on behalf of the Controller, process information regarding:	Yes	No
racial or ethnic origin, or political, philosophical or religious beliefs,		N
that a person has been suspected of, charged with or convicted of a criminal offence,		N
health information,	Y	
sexual orientation,		N
trade union membership	Y	
genetic or biometric data		N

**Appendix B - Overview current subcontractors**

Current subcontractors of the Processor with access to the Controller's Personal Data upon signing this Agreement include:

<b>Name</b>	<b>Location/country</b>	<b>Legal transfer mechanism if the subcontractor has access to personal data from countries outside the EU</b>	<b>Assisting the Processor with</b>
Visma ITC AS	Oslo, Norway	Not applicable within EU	Storage on servers