Data Processing Agreement

This Data Processing Agreement forms part of the Terms of Service or other written or electronic agreement between the Customer (“Controller”) and SmartDok AB (“SmartDok” or “Processor”) for the purchase and/or demonstration of services from SmartDok to reflect the Parties agreement with regard to Processing of Personal Data.

1. Introduction

1.1. Both Parties confirm that the undersigned has 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:

- *Terms of Sevice (Brukervilkår)*

1.2. If the Controller changes the contact person(s), the Processor must be informed of this in writing.

2. Definitions

2.1. 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 EU 2016/679 General Data Protection Regulation (“GDPR”).

3. Scope

3.1. 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 organizational measures according to applicable privacy legislation, including the GDPR.

3.2. The purpose behind the Processor’s Processing of Personal Data on behalf of the Controller is to fulfill the Service Agreement(s).

3.3. This Agreement takes precedence over any conflicting provisions regarding the Processing of Personal Data in the Service Agreements or in other former agreements or written communication between the Parties. This Agreement is valid for as long as agreed in Appendix A.

4. The Processor’s rights and obligations

4.1. The Processor shall only Process Personal Data on behalf of and in accordance with the Controller’s written 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.

4.2. 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.

4.3. The categories of Data Subjects and Personal Data subject to Processing according to this Agreement are outlined in Appendix A.

4.4. The Processor shall ensure the confidentiality, integrity, and availability of Personal Data are according to the privacy legislation applicable to The Processor. The Processor shall implement systematic, organizational, 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.

4.5. The Processor shall assist the Controller by appropriate technical and organizational 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 the request from Data Subjects, and general privacy compliance under the GDPR article 32 to 36.

4.6. 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, the Processor may charge the Controller for such request for additional services.

4.7. 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.

4.8. 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 privacy 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

4.9. The Processor shall ensure that persons that have the right to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.10. The Processor will not respond directly to requests from Data Subjects unless authorized 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.

4.11. 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.

4.12. The Processor might Process Personal data about users and the Controller's use of the service when it is necessary to obtain feedback and improve the service. The Controller grants the Processor the right to use and analyze aggregated system activity data associated with your use of the Services for the purposes of optimizing, improving, or enhancing the way the Processor provides the services and to enable the Processor to create new features and functionality in connection with the services. SmartDok shall be considered the Controller for such processing and the processing is therefore not subject to this Agreement.

4.13. When using the service, the Controller will add data to the Software ("Customer Data"). The Controller acknowledges and does not object to the Processor using Customer Data in an aggregated and anonymized format for improving the services delivered to customers, research,

training, educational, and/or statistical purposes.

5. The Controller's rights and obligations

5.1. The Controller confirms by the signing of this Agreement that:

- The Controller has the legal authority to process and disclose to the Processor (including any subprocessors used by the Processor) the Personal Data in question.
- The Controller has the responsibility for the accuracy, integrity, content, reliability and lawfulness of the Personal Data disclosed to the Processor.
- The Controller has fulfilled its duties to provide relevant information to Data Subjects and authorities regarding the processing of Personal Data according to mandatory data protection legislation.
- 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.

6. Use of subprocessors and transfer of data

6.1. As part of the delivery of services to the Controller according to the Service Agreements and this Agreement, the Processor will make use of subprocessors and the Controller gives its general consent to the usage of subprocessors. Such subprocessors can be other companies within the Visma group or external third-party subprocessors. All subprocessors are included in Appendix B. The Processor shall ensure that subprocessors agree to undertake responsibilities corresponding to the obligations set out in this Agreement.

6.2. An overview of the current subprocessors with access to Personal Data can be found in the Visma Trust Centre on this web site: https://www.visma.com/trust-centre/product-search/ . The Processor may engage other EU/EEA located companies in the Visma Group as subprocessors without the Visma company being listed at Trust Center and without prior approval or notification to the Controller. This is usually for the purposes of development, support, operations etc. The Controller may request more detailed information about subprocessors.

6.3. If the subprocessors are located outside the EU or the EEA, the Controller gives the Processor authorization to ensure proper legal grounds for the transfer of Personal Data out of the EU /EEA on behalf of the Controller, hereunder by entering into EU Standard Contractual Clauses (SCCs).

6.4. The Controller shall be notified in advance of any changes in subprocessors that Process Personal Data. If the Controller objects to a new subprocessor within 30 days after a notification is given, the Processor and Controller shall review the documentation of the Subprocessor's compliance efforts in order to ensure fulfillment of applicable privacy legislation. If the Controller still objects and has reasonable grounds for this, the Controller can not reserve themselves against the use of such a subprocessor (due to the nature of online standard Software in particular), but the Customer may terminate the Service Agreement for which the subprocessor in dispute is being used for.

7. Security

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

7.2. The Service Agreement sets forth the measures or other data security procedures that the Processor implements in the Processing of Personal Data. The Controller shall be responsible for the appropriate and adequate security of the equipment and the IT environment under its responsibility

8. Audit rights

8.1. 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 upon 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.

8.2. 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.

8.3. 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.

8.4. The Controller shall be responsible for any costs arising from the Controller's requested audits. Requests for assistance from the Processor may be subject to fees.

9. Term and termination

9.1. This Agreement is valid for as long as the Processor processes Personal Data on behalf of the Controller after the Service Agreements or as otherwise agreed in Appendix A.

9.2. 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. Such deletion will take place as soon as reasonably practicable unless EU or local law requires further storage. 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.

10. Changes and amendments

10.1. Changes to the Agreement shall be signed by both Parties in order to be valid.

10.2. 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.

11. Liability

11.1. For the avoidance of doubt, the Parties agree and acknowledge that each Party shall be liable for and held accountable to pay administrative fines and damages directly to data subjects which the Party has been imposed to pay by the data protection authorities or authorized courts according to applicable privacy legislation. Liability matters between the Parties shall be governed by the liability clauses in the Service Agreement between the Parties.

12. Governing law and legal venue

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

Appendix A - Data subjects, Types of personal data, Purpose, Nature, Duration

A.1 Categories of Data Subjects

- customer end users
- customer employees
- customer contact persons

A.2 Categories of Personal Data

- contact information such as name, phone, address, email, etc.
- job information such as position, company, etc
- economical information such as salary, hours of work etc.

A.3 Special categories of Personal Data (Sensitive Personal Data)

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,		x
health information,		x
sexual orientation,		x
trade union membership		x
genetic or biometric data		x

A.4 Purpose of the processing

The purpose of the data processor's processing of personal data on behalf of the data controller is:
Delivering services in accordance with the Service Agreement.

A.5 Nature of the processing

The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):
storing/hosting, registering, testing, changing/editing, reporting, sending.

A.6 Duration of the processing:

The duration of the processing of personal data is 12 months after termination of the Service Agreements.

Appendix B - Overview of subprocessors

The subprocessors of the Processor with access to the Controller's Personal Data are found always up to date on: https://www.visma.com/trust-centre/product-search/

The Processor may engage other EU/EEA-located companies in the Visma Group as subprocessors without the Visma company being listed above and without prior approval or notification to the Controller. This is usually for the purposes of development, support, operations, etc.