Data Processing Agreement

Last Version: 14. February 2024

Following Data Processing Agreement is for the purposes of Article 28(3) of Regulation 2016/679 (“the GDPR”), and is applicable between Visiodocs ApS, with company registration number 39577550, located at Bombakken 41, 3320 Skævinge, Denmark as the data processor (“data processor”), and Visiodocs’ customer who uses the free version of the Visiodocs Document Management Solution as the data controller (“data controller”). Each a ‘party’; together ‘the parties’.

When using the free version of the Visiodocs Document Management Solution the data controller, together with the data processor, agrees on the following Data Processing Clauses (“the Clauses”) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

We may update these Terms from time to time. The expired versions will be available here on our website.

Table of Contents

1. Preamble

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

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of Visiodoc's SaaS (Software as a Service) the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements 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 controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions 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 data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. 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.

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

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

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

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

6. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 7 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7. Transfer of data to third countries or international organisations

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

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

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

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

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

8. Assistance to the data controller

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

    This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

    a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

    b. the data controller's obligation to 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 controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

    d. the data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

9. Notification of personal data breach

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

2. The data processor's notification to the data controller shall, if possible, take place within 72 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10. Erasure and return of data

1. On termination of the provision of personal data processing services, the data controller deletes all personal data, and thereby the data is also deleted at the data processor. If the data processor otherwise has processed personal data stored, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

11. Responsibility

1. The parties are liable for damages under the general rules of Danish law, however, none of the parties is entitled to claim compensation for indirect loss or consequential damages, regardless of whether it is the Data Controller, the Data Processor or a third party, who suffer these indirect losses or consequential damages. Loss of business opportunity, loss of profits, operating loss, loss of revenue, loss of goodwill, loss of data, including losses in connection with the restoration of data shall always be considered as indirect loss/consequential damages.

2. The data processor's total liability under these Clauses is limited in total to an amount equal to the remuneration paid by the Data Controller to the Data Processor within 3 months prior to the event that may have triggered a claim for compensation or compensation.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

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

13. The parties' agreement on other terms

1. The parties may agree 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.

14. Commencement and termination

1. The Clauses shall become effective automatically when the data controller uses the Visiodocs Document Management Solution.

2. The Clauses apply for as long as the data controller uses the free version of the Visiodocs Document Management Solution, and the Clauses cannot be terminated under this duration unless other Clauses governing the processing activities have been agreed between the parties.

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The data processor provides the data controller with a platform that can be used for viewing and document management.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The data processor provides a SaaS-solution for document management.

Processing includes, according to detailed instructions from the data controller, storing/viewing/annotating/encrypting documents that potentially contain personal data. The documents are instructed (provided) by the data controller by transferring data from the data controller's own data stores. The data processor only processes personal data authorised by the data controller.

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

The data processor only processes personal data that appears in the documents provided by the data controller.

It is not possible to delimit the type of personal data that the processing may include, as the type of personal data depends on the documents provided by the data controller. This can be ordinary personal data, sensitive personal data or confidential personal data.

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

The category of data subjects may include customers, employees, business partners and other third parties who may appear in the processed documents.

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

The processing is not limited in time. The data processor processes personal data on behalf of the data controller for the duration of the contract between the parties.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

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

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Google Ireland Ltd.		Google Building Gordon House, Barrow St, Dublin 4, Ireland	Storing of data
I love PDF		c/ Sabino Arana 60, 08028 Barcelona (Spain)	Converting MS Office files to PDF Open password protected PDF files

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Appendix C Instruction pertaining to the use of personal data

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

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data controller uploading documents to the data processor's SaaS solution. Such uploaded documents may contain personal data.

The processing therefore consists of the collection, storage and processing of documents containing personal data.

C.2. Security of processing

The level of security shall take into account:

The processing involves a large number of personal data, or documents which may include personal data covered by Article 9 of the General Data Protection Regulation on "sensitive personal data", which is why a high level of security must be established.

The data processor is then entitled and obliged to make decisions on which technical and organisational security measures to implement in order to establish the necessary (and agreed) security level.

The data processor's implemented security measures are described in Visiodoc's Technical Review, which is available upon request (info@visiodocs.com). The document provides a detailed description of the implemented security measures, which include (but are not limited to):

- Established procedures and policies that ensure data protection
- Access management
- Access control
- Vulnerability management and security in development and support processes
- Security updates of systems in use
- Security requirements for information systems
- Encryption
- Automatic backup

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures.

C.3.1: About data breach

The data processor must immediately identify and confirm that a personal data breach has indeed occurred. This may involve examining log files, monitoring data or other relevant sources to verify the incident.

The data processor must also inform the data controller of the personal data breach without undue delay. This allows the data controller to take appropriate measures and to notify the competent supervisory authority in a timely manner, cf. Article 33 of the GDPR.

The data processor shall assist the data controller by having an incident response plan in place (Visiodocs Information Security Incident Procedure).
The data processor shall initiate an investigation and analysis of the personal data breach to determine the cause, scope and possible consequences of the incident. This may involve technical investigations, review of log files and co-operation with relevant authorities or third parties as necessary.

The data processor must actively contribute to remedying the personal data breach and implement necessary measures to prevent recurrence. This may include closing security gaps, updating systems, strengthening access controls, changing passwords and other technical or organisational measures.

C.3.2: About request from the data subject

The data processor has implemented and follows policies and procedures that ensure that appropriate aspects of good security practices are enforced so that the data processor is able to assist the data controller in a timely manner, including to ensure that the rights of data subjects are met.

The data processor has established and will maintain procedures and technical functions that allow the data processor, at the request of the data controller, to (i) identify personal data relating to data subjects so that the data controller can fulfil requests for access to data from data subjects, (ii) rectify or erase stored personal data and (iii) restrict the further processing of personal data.

C.3.3: Regarding other assistance

At the data controller's request, the data processor shall - taking into account the nature of the processing and the information available to the data processor - assist the data controller to a reasonable extent - with input/contribution to the data controller's performance of its tasks and compliance with its obligations set out in Clauses 9.1 and 9.2.

C.4. Storage period/erasure procedures

Personal data is stored until the data controller deletes the data.

Upon termination of the service regarding the data processor's processing of personal data, the data processor shall either delete or return the personal data in accordance with Clause 10.1.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller’s prior written authorisation:

Processing of the personal data takes place at the data processor, at its address at any time, as well as at the data processor's sub-processors.

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

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

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

The data processor undertakes to respond once a year to the data controller's questions (e.g. in the form of a questionnaire) regarding the data processor's data processing with descriptions of controls aimed at data protection, processing of personal data and technical and organisational measures.

The data controller or a representative of the data controller has in addition or as an alternative access, by agreement, to conduct an annual physical inspection of the premises from which the data processor carries out the processing of personal data, including physical

premises and systems used for or in connection with the processing, in order to determine the data processor's compliance with the GDPR, data protection provisions in other EU law or the national law of the Member States and these provisions.

In addition to the planned supervision, the data controller may carry out an inspection at the data processor's premises when the data controller deems it necessary. The controller must give at least 30 days' notice.

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

The data processor shall annually obtain an audit report from an independent third party regarding the sub-processor's compliance with the GDPR, data protection provisions in other Union or Member State law and these Clauses.

Where an audit from an independent third party is not deemed necessary or where it is not possible, the data processor may annually submit a questionnaire to the sub-processor regarding its data processing with descriptions of controls aimed at data protection, processing of personal data and technical and organisational measures.