

Addition to the CleanManager subscription agreement

# Data Processing Agreement

## Standard Contractual Clauses

in accordance with of Article 28(3) of Regulation 2016/679 (the GDPR) for the purpose of the data processor's processing the personal data.

These standard contractual clauses (the Clauses) are an addition to the CleanManager subscription agreement (hereinafter the "Application") between the Parties, based on the at any time applicable terms and conditions for the Application, and form an integral part thereof.

The Clauses are accepted by checking "*I hereby confirm that I have read and accepted the terms and conditions for the use of CleanManager*" on the order form and apply between the following parties:

**Customer, who accepts the terms and conditions for the Application**

(the "data controller")

and

**CleanManager ApS  
CVR 39 23 09 92  
Holkebjergvej 74  
5250 Odense SV  
Denmark**

(the "data processor")

each a "party"; together "the parties"

These Clauses were last revised on 30 March 2023.

# 1 Table of Contents

2 Preamble.....	3
3 The rights and obligations of the data controller.....	4
4 The data processor acts according to instructions.....	4
5 Confidentiality.....	4
6 Security of processing.....	5
7 Use of sub-processors.....	6
8 Transfer of data to third countries or international organisations.....	7
9 Assistance to the data controller.....	7
10 Notification of personal data breach.....	9
11 Erasure and return of data.....	9
12 Audit and inspection.....	10
13 The parties' agreement on other terms.....	10
14 Commencement and termination.....	10
15 Data controller and data processor contacts/contact points.....	11
Appendix A Information about the processing.....	12
Appendix B Authorised sub-processors.....	14
Appendix C Instruction pertaining to the use of personal data.....	15
Appendix D The parties' terms of agreement on other subjects.....	18

## 2 Preamble

- 2.1 These Contractual Clauses (the 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.
- 2.2 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).
- 2.3 In the context of the provision of subscription for the application CleanManager (hereinafter "the Application"), the data processor will process personal data on behalf of the data controller in accordance with the Clauses.
- 2.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
- 2.5 Four appendices are attached to the Clauses and form an integral part of the Clauses.
- 2.6 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.
- 2.7 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.
- 2.8 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.
- 2.9 Appendix D contains provisions for other activities which are not covered by the Clauses.
- 2.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
- 2.11 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.

### **3 The rights and obligations of the data controller**

- 3.1 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<sup>1</sup> data protection provisions and the Clauses.
- 3.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
- 3.3 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.

### **4 The data processor acts according to instructions**

- 4.1 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.
- 4.2 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.

### **5 Confidentiality**

- 5.1 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.
- 5.2 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.

---

<sup>1</sup> References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

## 6 Security of processing

6.1 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.

6.2 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.

6.3 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Article 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.

## **7 Use of sub-processors**

- 7.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
- 7.2 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.
- 7.3 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 two (2) months 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.
- 7.4 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.

- 7.5 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.
- 7.6 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.

## **8 Transfer of data to third countries or international organisations**

- 8.1 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.
- 8.2 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.
- 8.3 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
- 8.4 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.
- 8.5 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.

## **9 Assistance to the data controller**

- 9.1 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

9.2 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, the Danish Data Protection Agency ("Datatilsynet"), 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, the Danish Data Protection Agency ("Datatilsynet"), 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.

9.3 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.

## **10 Notification of personal data breach**

10.1 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.

10.2 The data processor's notification to the data controller shall, if possible, take place within 36 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.

10.3 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.

10.4 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.

## **11 Erasure and return of data**

11.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

## **12 Audit and inspection**

- 12.1 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.
- 12.2 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.
- 12.3 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**

- 13.1 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**

- 14.1 The Clauses shall become effective by accepting the terms and conditions for the use of the Application.
- 14.2 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.
- 14.3 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.
- 14.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

## 15 Data controller and data processor contacts/contact points

15.1 The data controller can contact the data processor using the following contact:

**Name:** Jakob Witte Larsen  
**Position:** Head of development and responsible for personal data  
**Telephone:** + 45 60 95 03 48  
**E-mail:** jwl@cleanmanager.com

15.2 The data processor can contact the data controller via the contact person specified in the Application (CleanManager). It is the responsibility of the data controller at all times to ensure that the contact information is kept up-to-date in the Application.

## **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 purpose of the data processor's processing of personal data on behalf of the data controller is so that the data controller can use the Application (CleanManager), which is owned and operated by the data processor, to manage and plan work on the data controller's employees and customers.

### **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)**

Delivering, operating and further developing of the Application, including storing data and backup management.

Besides storing of data, the processing may also in – accordance with the data controllers instruction – include:

- Processing of data in connection with import of customer data.
- Access to data in connection with support in order to assist the customers with issues in relation to the use of the Application.

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

**For employees:** Name, address, phone no., email, CPR-no., bank statements, employment and termination date, emergency contact person, picture, time and place of meetings, employment contract, workplace assessments etc.

**For customers:** Name, billing and shipping address, phone no., email, CVR-no. and EAN-no., CPR-no., information on contact person (name, phone no. and email), contracts, work assessments etc.

The data processor does not support the recording of data related to the special categories of personal data, including health, race and ethnicity and personal data related to criminal conviction and offences.

### **A.4 Processing includes the following categories of data subject**

The processing may include the following categories of data subjects insofar the data on these categories are entered into the Application:

- I. The data controller's current employees
- II. The data controller's terminated employees
- III. The data controller's potential customers and their contact persons
- IV. The data controller's current customers and their contact persons
- V. The data controller's previous customers and their contact persons

Section III to V includes both private persons, enterprises and public organisations.

**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 may be performed for the entire and continuous duration of the subscription period and 30 days after the termination of the subscription period.

There may be a duration of 20 days from the period of deletion until the data is deleted from the backup systems.

## 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/Org.no.	Address	Description of processing
Sentia Solutions A/S	10 00 81 23	Smedeland 32 2600 Glostrup	Server operation, hosting and backup
ScanNet A/S	29 41 20 06	Højvangen 4 8660 Skanderborg	Server operation and backup
Compaya A/S	31 37 54 28	Palægade 4, 2. tv. 1261 København K	SMS relay
Sendinblue SAS	498 019 298	7 rue de Madrid 75008 Paris, France	E-mail and SMS relay
Zendesk, Inc.	N/A	1019 Market Street, 6th Floor San Francisco, California 94103	Support (Email, chat, etc.)
Video Communication Services AS	918 470 573	Gate 1, no. 101, 6700 Maaloy, Norway	Support (Video conference)

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.

### B.2 Prior notice for the authorisation of sub-processors

Insofar the data controller has any objections for the use of a sub-processor, the data controller shall notify the data processor in this regard within two (2) weeks after receiving the notification from the data processor. The data controller may only object insofar the data controller has reasonable and specific reasons hereto.

## **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 processor performing the following:

The data processor performs delivery, operation and further development of a cleaning service application (CleanManager), including storing of data and backup management, on behalf of the data controller.

### **C.2 Security of processing**

The level of security shall take into account:

The processing concerns a limited amount of personal data which does not include "special categories of personal data" in relation to Article 9 GDPR, in which relation the level of security shall be organised.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

The data processor, in collaboration with the sub-processors, establishes adequate technical security measures to ensure that data is stored and transmitted securely, including data encryption, network segmentation and server monitoring. These are evaluated on an ongoing basis based on the risk assessment. Servers and workstations with access to personal data use either Linux or Mac OSX as the operating system, and are continuously updated.

The data processor carries out internal checks on its management. Employees are trained in processing personal data in connection with start-up, as well as once a year, and are only granted access to customer data if they have a work-related need for this.

The Data Processor performs continuous deletion procedures which ensure that data is not stored for longer than stipulated in the Clauses. In addition, guides have been prepared for data controllers on how data can be deleted and anonymized in the system.

The data processor audits relevant sub-data processors in connection with regular checks and audits, where it is assessed whether the sub-processors comply with the

data processor's own and the data controller's requirements as well as requirements from laws, regulations or supervisory organisations.

The data processor conducts ongoing awareness training with employees to ensure that security breaches can be quickly identified at the data processor. In case of any security breaches, such as data leaks or hacking, the data processor has prepared a security procedure for handling this which ensures proper notification of the breach to the data controllers.

The data processor issues an annual statement of assurance from an independent auditor based on the ISAE-3000 standard, or another appropriate standard, which provides a transparent and fair view of the data processor's compliance with these Clauses and the protection of the data controller's personal data. The data processor's specific security measures will be further set out in the annual ISAE 3000 statement, which will be made available to the data controller at their request.

### **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:

Insofar as possible, the data processor shall assist the data controller in responding to requests from data subjects in connection with the use of the Application and assist the data controller in preparing risk assessments and implementing appropriate security measures, notifying the Danish Data Protection Agency (“Datatilsynet”) and the data subjects in the event of security breaches, preparing data protection impact assessments and conducting prior consultation of the Danish Data Protection Agency (“Datatilsynet”) with processing carried out with the Application.

### **C.4 Storage period/erasure procedures**

Personal data is stored at the data processor until the data controller request to have the data erased or returned. In connection with the termination of the subscription for the Application, data shall be deleted after 30 days after unless the data controller requests otherwise.

There may be a duration of 20 days from the period of deletion until the data is deleted from the backup systems.

### **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:

The data processor’s above stated address and the addresses of the sub-processors as described in Appendix B.



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

In connection with the operation of the Application and as described in Appendix B, a few number of sub-processors are used outside the EU. These sub-processors are based in the USA and have entered into standard contractual provisions for transmission to third countries, which means that the sub-processor can ensure an adequate level of security and protection. With the acceptance of the Regulations, the data controller has approved the transfer of personal data to the sub-processors used in Appendix B.

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 shall once a year with a maximum of 12 months gap obtain an audit report from an independent third party regarding the description of controls relating to data protection and processing of personal data in connection with the Clauses and related appendices.

The audit report is henceforth of the ISAE 3000 type 2 standard and contains both the data processor and any sub-processors' processing of personal data. The report shall be sent as soon as possible to the data controller after having been obtained.

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

The data controller's auditing of any sub-processors is done - as a starting point - through the data processor. The data processor continuously obtains a statement of assurance from an independent auditor from all relevant sub-processors, which can be made available at the request of the data controller.

## **Appendix D The parties' terms of agreement on other subjects**

### **D.1 Specification of the data processor's deletion**

The data processor must, in accordance with the provisions of the Clauses clause 11.1. ensure that any sub-processors also comply with the data processor's obligations regarding the deletion of personal data.

If the data controller does not instruct the data processor otherwise, the database belonging to a subscription will be deleted 30 days after the termination of the subscription and these Clauses. The data controller's data is stored during this period to ensure the possibility of reopening the subscription within a reasonable cancellation period.

The data processor shall submit - at the request of the data controller - documentation that the required deletion, cf. clause 11.1., has been made.

### **D.2 The data processor's remuneration**

The data controller remunerates the data processor separately for time and material spent in order to handle queries and tasks in accordance with the provisions of the Clauses, par. 9.1, 9.2, 10.3, 11.1, 12.1 and Appendix C, par. C.3 and C.7, which exceeds the data processor's general obligations in accordance with the applicable legislation. The remuneration is determined according to the data processor's current hourly rate available at CleanManager.com.

### **D.3 Changes and transfer of the Clauses**

The data processor and the data controller may at any time, with a prior notice of at least 30 calendar days, make changes to the Clauses. The change process and costs must be agreed in writing between the data processor and the data controller in accordance with the terms of the subscription conditions. In case of such changes, the data processor must ensure that the sub-processors are also bound by the changes without undue delay.

The data processor may assign its rights and obligations under the Clauses without the consent of the data controller, provided that to whom the rights and/or obligations are transferred is required to process personal data in accordance with the requirements applicable to the data processor, in according with the Clauses.