>Virksomhedsnavn<

**CONTRACTUAL CLAUSES**

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR) in relation to the data processor’s assessment of personal data.

**STANDARD
CONTRACTUAL CLAUSES**

**Between:**

|  |  |
| --- | --- |
| **Data processor** Mindmill Denmark ApS(Hereafter, "the data processor ")CVR: 32478298 Hasselager Centervej 21 - 23 8260 Viby J**&****Data controller** Virksomhed(Hereafter, "the data controller")CVR: xxAdressePostnummer og by  |  |

(individually called a ”party” and together ”the parties”)

Have agreed on the following Contractual Clauses (hereafter “the Clauses”) regarding the data processor’s management of personal data on behalf of the data controller.

**TABLE OF CONTENTS**

[1. Preamble 3](#_Toc95209604)

[2. The rights and obligations of the data controller 3](#_Toc95209605)

[3. The data processor acts according to instructions 4](#_Toc95209606)

[4. Confidentiality 4](#_Toc95209607)

[5. Security of processing 4](#_Toc95209608)

[6. Use of sub-processors 5](#_Toc95209609)

[7. Transfer of data to third countries or international organisations 6](#_Toc95209610)

[8. Assistance to the data controller 6](#_Toc95209611)

[9. Notification of personal data breach 7](#_Toc95209612)

[10. Erasure and return of data 8](#_Toc95209613)

[11. Audit and inspection 8](#_Toc95209614)

[12. The parties’ agreement on other terms 8](#_Toc95209615)

[13. Commencement and termination 8](#_Toc95209616)

[14. Data controller and data processor contact/ contacts points 9](#_Toc95209617)

[Appendix A - Information about the processing 10](#_Toc95209618)

[Appendix B - Authorised sub-processors 11](#_Toc95209619)

[Appendix C - Instruction pertaining to the use of personal data 12](#_Toc95209620)

# 1. PREAMBLE

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. 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 connection to the provision of a marketing automation system which generates leads on social media and where the data processor then processes the incoming leads on behalf of the data controller in accordance with the Clauses.
4. The Clauses must take priority over any similar provisions contained in other agreements between the parties.
5. Three 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, a description of 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. The Clauses along with appendices must be retained in writing, including electronically, by both parties.
10. The Clauses must not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or any 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]](#endnote-1) data protection provisions and the Clauses.
2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
3. The data controller must 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 must 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 must 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 must always be documented and kept in writing, including electronically, in connection with the Clauses.
2. The data processor must 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 must 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 must 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 must consequently not be accessible anymore to those persons.
2. The data processor must at the request of the data controller demonstrate that the concerned persons under the data processor’s authority are subject to the abovementioned duty of 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 must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller must 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:

1. Pseudonymisation and encryption of personal data;
2. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
5. According to Article 32 GDPR, the data processor must 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 must provide the data processor with all information necessary to identify and evaluate such risks.
6. Furthermore, the data processor must 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 requires further measures to be implemented than those already implemented by the data processor, the data controller must specify these additional measures to be implemented in Appendix C.

# 6. USE OF SUB-PROCESSORS

1. The data processor must meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
2. The data processor must therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without 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 must inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 90 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. When 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 must 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 for the sub-processor 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 must 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.

1. A copy of such a sub-processor agreement(s) and subsequent amendments must – 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(s), must not require submission to the data controller.
2. The data processor must agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller must be a third-party beneficiary to the sub-processor agreement and must 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.
3. If the sub-processor does not fulfil his data protection obligations, the data processor must 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.

# 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 must only occur on the basis of documented instructions from the data controller and must always take place in compliance with Chapter V of the 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 must 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 scope of the Clauses:
4. transfer personal data to a data controller or a data processor in a third country or in an international organization
5. transfer the processing of personal data to a sub-processor in a third country
6. have the personal data processed in by the data processor in a third country
7. 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, must be set out in Appendix C.6.
8. The Clauses must not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and these Clauses cannot be relied upon by the parties as a transfer tool under Chapter V of the GDPR.

# 8.  ASSISTANCE TO THE DATA CONTROLLER

1. Taking into account the nature of the processing, the data processor assists the data controller with 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 of the GDPR.

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

1. the right to be informed when collecting personal data from the data subject
2. the right to be informed if personal data have not been obtained from the data subject
3. the right of access
4. the right to rectification
5. the right to erasure (‘the right to be forgotten’)
6. the right to restriction of processing
7. notification obligation regarding rectification or erasure of personal data or restriction of processing
8. the right to data portability
9. the right to object
10. the right not to be subject to a decision based solely on automated processing, including profiling
11. In addition to the data processor’s obligation to assist the data controller pursuant to Clause 6.3., the data processor must 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:

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 supervisory authority: “Datatilsynet”, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

1. the data controller’s obligation to communicate the personal data breach to the data subject without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
2. 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);
3. the data controller’s obligation to consult the competent supervisory authority, the Danish supervisory authority: “Datatilsynet”, prior to processing if 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.
4. In Appendix C, the parties must define 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 must, 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 must, if possible, take place within 12 hours after the data processor has become aware of the personal data breach in order to enable the data controller to comply with the data controller’s obligation to inform about the personal data breach to the competent supervisory authority, cf. article 33 of the GDPR.
3. In accordance with Clause 9(2)(a), the data processor must 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, must be stated in the data controller’s notification to the competent supervisory authority:
4. The nature of the personal data including when possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
5. the likely consequences of the personal data breach;
6. the measures taken or proposed to be taken by the controller to address the personal data breach, including, when appropriate, measures to mitigate its possible adverse effects.
7. The parties must 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 processor is obliged to return all the personal data to the data controller and delete existing copies - at the expense of the data processor - unless Union or Member State law requires storage of the personal data.

# 11. AUDIT AND INSPECTION

1. The data processor must 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 must 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.

# 12. 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 with the Clauses or weaken the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

# 13. COMMENCEMENT AND TERMINATION

1. The Clauses must become effective on the date of both parties’ signature.
2. Both parties must be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.
3. The Clauses apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.
4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.
5. Signature

|  |  |
| --- | --- |
| **Data processor** Mindmill Denmark ApSCVR: 32478298 Hasselager Centervej 21 - 23 8260 Viby JDato: 24. marts 2022Underskrift  | **Data controller** VirksomhedCVR: xxAdressePostnummer og byDato: Underskrift |

# 14. DATA CONTROLLER AND DATA PROCESSOR CONTACT/ CONTACTS POINTS

1. The parties may contact each other using the following contact/contacts points:

**Data controller**

Name:

Position:

Telephone:

E-mail:

**Data processor**

Name: Janus Helkjær

Position: Lead Web Developer

Telephone: 2371 4902

E-mail: jh@mindmill.dk

1. The parties are under obligation to continuously inform each other of changes to contact/contacts points.

# 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:**

To set up a marketing automation system in order to generate leads on social media and then process all incoming leads on behalf of the data controller.

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

Leads which are generated through social media are sent to the Marketing Automation system using Zapier. From the Marketing Automation system, the data is transferred into a Google Lead Sheet. Leads are processed in the Marketing Automation system with e-mails and each action assigns a lead point in the system. In this case, regular personal data used (see A.3).

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

* Name
* E-mail
* Telephone
* Company
* Is signed up to receive a marketing lead

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

* Clients
* Clients’ employees

**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:**

As long as the specific lead does not unsubscribe or requests to be deleted from the database.

# 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** |
| Zapier |   | 548 Market St #62411, San Francisco, California 94104, USA | Sending data from advertising channels to ActiveCampaign and Google |
| Google LLC |   | 1600 Amphitheatre Parkway, Mountain View, California 94043, USA | Is used for lead sheet from which the data controller’s salespeople work. |
| DigitalOcean, LL |   | 101 Avenue of the Americas, New York 10013, USA | At their servers in Frankfurt, we host websites and campaign sites. |
| ActiveCampaign, LLC |   | 1 North Dearborn St5th FloorChicago, IL 60602, USA | ActiveCampaign is used for storage of contact information of leads and automated marketing activities. |

On the commencement of the Clauses, the data controller must authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor must 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.

All sub-processors have signed the Standard Contractual Clauses at the processor’s.

# 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 must be carried out by the data processor performing the following:

Leads that are generated through social media are sent to a Marketing Automation system using Zapier. From the Marketing Automation system, the data is transferred to a Google Lead Sheet. The leads are processed in the Marketing Automation system with e-mails, and each action is awarded with a lead point in the system.

**C.2. Security of processing**

The level of security must take into account:

The data processor must 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 processing involves personal data which is subject to article 6 of the GDPR and accordingly the level of security must be established.

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

Excerpt from the data processor’s description of current safety measures:

* + We use Google Drive Business (cloud) for storage of data applying both to our own and our clients’ data
	+ We have upgraded to the Business version for increased safety and control measures.
	+ All access is controlled centralized by the management, and we can shut down all access immediately in case of a security breach (theft, hacking, etc.).
	+ We have full surveillance and history of all behavior.
	+ Furthermore, we have implemented double opt-in on all access points so you have to receive a text message if you sign on from a not authorised unit - besides, the administration will be informed. This makes sure that unauthorised personnel cannot access our systems and our data.
	+ Additionally, everything is structured in a such a way that the individual employee always only has access to the necessary system and data in order for him or her to do his job - and nothing further.
	+ All emplyees are instructed in correct dealings with data, breach of security procedures, etc.
	+ All our computers are encrypted and installed with a disk wiper. Therefore, if a computer should get stolen, we can be 100% sure that unauthorised people will not access our data since the computer is completely wiped as soon as it is opened and/or the hard drive is encrypted.

**C.3 Assistance to the data controller**

The data processor must 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.

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

Personal data is stored as long as the registered does not request to be erased.

Upon termination of the provision of personal data processing services, the data processor must either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller’s original choice. Such modification must be documented and kept in writing, including electronically, in connection with the Clauses.

**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:

Mindmill’s address in Viby - as stated in the Contractual Clauses.

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

Transfer of personal data to third countries only occur when standard contractual clauses have been signed. At all times, the data processor is obliged to follow new guidelines and revised versions of the standard contractual clauses performed by the European Commission.

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

**C.7 Procedures for the data controller’s audits, including inspections, of the processing of personal data**

Once a year, the data controller can obtain an inspection report at their own expense from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

On 14 days notice, the data controller has the right to perform a physical inspection of the locations from which the processing of personal data is carried out, including physical facilities as well as systems used for and related to the processing to ascertain the data processor’s compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data controller may perform an inspection of the data processor when the data controller finds it necessary.

The inspection report is forwarded without unnecessary delays to the data controller for information. The data controller can contest the scope of, and/or the methodology used, in the report, and in such cases, they can request a new inspection report in another scope and/or using a different method.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller’s expenses related to a physical inspection must be defrayed by the data controller. The data processor is, however, under the obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

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

No inspection reports have been scheduled.

In addition, the data processor or the data processor’s representative must have access to inspect, including physically inspect, the locations, from which the processing of personal data is carried out. Such inspections must be performed when the data processor (or the data controller) deems it required.

Without delay, documentation for such inspections must be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the inspection and may in such cases request a new inspection under a revised scope and/or different methodology.

The data processor’s and the sub-processor’s costs related to physical inspection at the sub-processor’s facilities must not concern the data controller – regardless of whether the data controller has initiated and participated in such inspection.

1. References to ”Member States” made throughout the Clauses must be understood as references to “EEA Member States”. [↑](#endnote-ref-1)