

Data Processing Agreement

Between

The Data Controller

Name: _____

Reg number: _____

Address: _____

Postal code: _____

City: _____

Country: _____

and

The Data Processor

NoviPOS ApS

Reg number: DK-39843943

Gjellerupvej 91a

8230 Åbyhøj

Denmark

1 Content

- 1 Content..... 2
- 2 Background for the data processing agreement..... 3
- 3 Obligations and rights of the controller 4
- 4 The data processor acts according to instructions..... 4
- 5 Confidentiality 4
- 6 Processing safety 4
- 7 Use of sub-processors 5
- 8 Transfer of data to third countries or international organisations 6
- 9 Assistance to the data controller 7
- 10 Notification of personal data breaches..... 8
- 11 Deletion and return of information..... 8
- 12 Supervision and audit..... 9
- 13 Parties' agreements on other matters 9
- 14 Entry into force and termination..... 10
- 15 Contact persons/contact points at the data controller and the data processor 11
- Appendix A.....Information about the processing..... 11
- Appendix B Conditions for the data processor's use of sub-processors and list of approved sub-processors 12
 - B.1 Conditions for the data processor's use of any sub-processors 12
 - B.2 Approved sub-processors..... 12
- Appendix CInstructions regarding the processing of personal data..... 13
 - C.1 Subject-matter/instructions 13
 - C.2 Processing safety 13
 - C.3 Storage period/deletion routine 13
 - C.4 Processing site 14
 - C.5 Instructions or approvals regarding the transfer of personal data to third countries..... 14
 - C.6 Detailed procedures for the data controller's supervision of the processing carried out by the data processor..... 14
 - C.7 Detailed procedures for the supervision of the processing carried out by any sub-processors 14
- Appendix D.....Adjustment of other matters by the parties..... 15
 - D.1 Assistance to the Data Controller: 15

1.1 Background for the data processing agreement

1. This Agreement sets out the rights and obligations that apply when the Processor carries out the processing of personal data on behalf of the Controller.
2. The agreement is designed with a view to the parties' compliance with Article 28(3) of *Regulation (EU) 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)*, which sets out specific requirements for the content of a data processing agreement.
3. The Data Processor's processing of personal data takes place for the purpose of fulfilling the parties' "main agreement": [Rental and Service Agreement].
4. The data processing agreement and the "main agreement" are interdependent and cannot be terminated separately. However, the data processing agreement can – without terminating the "main agreement" – be replaced by another valid data processing agreement.
5. This Data Processing Agreement takes precedence over any corresponding provisions in other agreements between the parties, including in the "Main Agreement".
6. This agreement includes four appendix. The appendix function as an integral part of the data processing agreement.
7. The Data Processing Agreement Appendix A contains details of the processing, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.
8. The Data Processing Agreement A.1 contains the data controller's conditions for the data processor to make use of any sub-processors, as well as a list of the sub-processors, if any, that the data controller has approved.
9. The Data Processing Appendix B contains detailed instructions on what processing the data processor must carry out on behalf of the data controller (the object of the processing), what security measures must be observed as a minimum, and how the data processor and any sub-processors are supervised.
10. The Data Processing Appendix C contains the parties' possible regulation of matters that are not otherwise stated in the data processing agreement or the parties' "main agreement".
11. This Data Processing Agreement does not release the Data Processor from obligations that are directly imposed on the Data Processor under the General Data Protection Regulation or any other legislation.

2 Obligations and rights of the controller

1. The data controller is generally responsible to the outside world (including the data subject) for ensuring that the processing of personal data takes place within the framework of the General Data Protection Regulation and the Data Protection Act.
2. The data controller therefore has both the rights and the obligations to make decisions about the purposes and means for which processing may be carried out.
3. The data controller is responsible, among other things, for ensuring that there is a legal basis for the processing that the data processor is instructed to undertake.

3 The data processor acts according to instructions

1. **The Data Processor may only process personal data on documented instructions from the Data Controller, unless required by Union or Member State law to which the Data Processor is subject; In that case, the processor shall inform the controller of this legal requirement prior to processing, unless the court in question prohibits such notification on grounds of important public interest, cf. Article 28(3)(a).**
2. **The data processor shall immediately notify the data controller if, in the opinion of the data processor, an instruction is in conflict with the General Data Protection Regulation or data protection provisions in other EU law or the national law of the Member States.**

4 Confidentiality

1. The data processor ensures that only those persons who are currently authorised to do so have access to the personal data processed on behalf of the data controller. Access to the information must therefore be shut down immediately if the authorisation is withdrawn or expires.
2. Only persons for whom it is necessary to have access to the personal data in order to fulfil the data processor's obligations to the data controller may be authorised.
3. **The Data Processor shall ensure that the persons authorised to process personal data on behalf of the Data Controller have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.**
4. The data processor must, at the request of the data controller, be able to demonstrate that the relevant employees are subject to the above-mentioned duty of confidentiality.

5 Processing safety

1. **The Data Processor shall implement all measures required under Article 32 of the General Data Protection Regulation**, which states, inter alia, that, taking into account the current level, the implementation costs and the nature, scope, context and purpose of the processing in question, as well as the risks of varying probability and severity to the rights and

freedoms of natural persons, appropriate technical and organisational measures must be implemented to ensure a level of security appropriate to these risks.

2. The above obligation entails that the data processor must carry out a risk assessment and then implement measures to address identified risks. These may include, as appropriate, the following measures:
 - a. Pseudonymization and encryption of personal data
 - b. Ability to ensure the ongoing confidentiality, integrity, availability and robustness of processing systems and services
 - c. Ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
 - d. A procedure for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the safety of treatment;
3. In connection with the above, the Data Processor must – in all cases – implement at least the level of security and the measures specified in more detail in Appendix C of this Agreement.
4. Any regulation/agreement between the parties on remuneration or the like in connection with the data controller's or data processor's subsequent requirement to establish additional security measures will be stated in the parties' "main agreement" or in Appendix D of this agreement.

6 Use of sub-processors

1. **The data processor must meet the conditions referred to in Article 28(2) and (4) of the General Data Protection Regulation in order to make use of another data processor (sub-processor).**
2. **Thus, the data processor may not make use of another data processor (sub-processor) for the performance of the data processing agreement without prior specific or general written approval from the data controller.**
3. **In the event of general written approval, the Processor shall notify the Controller of any planned changes regarding the addition or replacement of other Processors, thereby giving the Controller the opportunity to object to such changes.**
4. The data controller's detailed terms and conditions for the data processor's use of any sub-processors are set out in this agreement's A.1.
5. The Controller's possible approval of specific sub-processors is set out in the A.1.
6. **Where the Processor has the Controller's approval to make use of a sub-processor, the Processor shall ensure that the sub-processor imposes on the Sub-processor the same data protection obligations as those set out in this Data Processing Agreement, through a contract or other legal document under Union or Member State law, thereby providing**

in particular the necessary guarantees that the Sub-processor will implement the appropriate technical and organisational measures. measures in such a way that the processing meets the requirements of the General Data Protection Regulation.

The data processor is thus responsible for – through the conclusion of a sub-data processing agreement – to impose on any sub-processor at least the obligations that the data processor itself is subject to under the data protection rules and this data processing agreement and its appendices.

7. The sub-processing agreement and any subsequent amendments thereto are sent – at the request of the data controller – in a copy to the data controller, who thereby has the opportunity to ensure that a valid agreement has been entered into between the data processor and the sub-processor. Any commercial terms, e.g. prices, which do not affect the data protection law content of the sub-data processing agreement, do not need to be sent to the data controller.
8. In its agreement with the sub-processor, the data processor must include the data controller as a third party beneficiary in the event of the data processor's bankruptcy, so that the data controller can assume the data processor's rights and enforce them against the sub-processor, e.g. so that the data controller can instruct the sub-processor to delete or return data.
9. **If the sub-processor fails to fulfil its data protection obligations, the data processor remains fully liable to the controller for the fulfilment of the sub-processor's obligations.**

7 Transfer of data to third countries or international organisations

1. **The Processor may only process personal data on documented instructions from the Controller, including with regard to the transfer (disclosure, disclosure and internal use) of Personal Data to third countries or international organisations, unless required by Union or Member State law to which the Processor is subject; in which case the Processor shall inform the Controller of this legal requirement prior to processing; unless the court in question prohibits such notification on grounds of important public interest, cf. Article 28(3)(a).**
2. Without the data controller's instructions or approval, the data processor can therefore - within the framework of the data processing agreement - among other things;
 - a. disclose the personal data to a data controller in a third country or in an international organisation;
 - b. entrust the processing of personal data to a sub-processor in a third country;
 - c. have the data processed in another of the data processor's departments located in a third country.
3. Any instructions or approval by the Controller to transfer personal data to a third country will be set out in the terms of this Appendix B.

8 Assistance to the data controller

1. **The data processor, taking into account the nature of the processing, assists the data controller as far as possible by means of appropriate technical and organisational measures, in fulfilling the data controller's obligation to respond to requests for the exercise of the data subjects' rights as laid down in Chapter 3 of the General Data Protection Regulation.**

This means that the data processor must, as far as possible, assist the data controller in connection with the data controller's compliance with:

- a. the duty to provide information when collecting personal data from the data subject;
 - b. the duty to provide information if personal data has not been collected from the data subject;
 - c. The data subject's right of access
 - d. the right to rectification;
 - e. the right to erasure ('right to be forgotten');
 - f. the right to restriction of processing;
 - g. Duty to notify in connection with rectification or erasure of personal data or restriction of processing
 - h. The right to data portability
 - i. the right to object
 - j. the right to object to the outcome of automated individual decisions, including profiling;
2. **The data processor assists the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32-36 of the General Data Protection Regulation, taking into account the nature of the processing and the information available to the data processor, cf. Article 28(3)(f).**

This means that the data processor, taking into account the nature of the processing, must assist the data controller in connection with the data controller ensuring compliance with:

- a. the obligation to implement appropriate technical and organisational measures to ensure a level of safety appropriate to the risks associated with the processing;
- b. the obligation to report a breach of personal data security to the supervisory authority (the Danish Data Protection Agency) without undue delay and, if possible, no later than 72 hours after the data controller has become aware of the breach, unless it is unlikely that the breach of personal data security entails a risk to the rights or freedoms of natural persons.
- c. the obligation to notify the data subject(s) of a personal data breach without undue delay when such a breach is likely to entail a high risk to the rights and freedoms of natural persons;
- d. the obligation to carry out a data protection impact assessment where a type of processing is likely to pose a high risk to the rights and freedoms of natural persons;

- e. the obligation to consult the supervisory authority (the Danish Data Protection Agency) before processing, where a data protection impact assessment shows that the processing will lead to a high risk in the absence of measures taken by the controller to limit the risk;
3. Any adjustments/agreements between the parties regarding remuneration or similar in connection with the data processor's assistance to the data controller will be set out in Appendix D of this agreement.

9 Notification of personal data breaches

1. The Data Processor notifies the Data Controller without undue delay after becoming aware that there has been a breach of personal data security at the Data Processor or any sub-processor.

If possible, the data processor's notification to the data controller must take place no later than [24 hours] after the data controller has become aware of the breach, so that the data controller has the opportunity to comply with any obligation to report the breach to the supervisory authority within 72 hours.

2. In accordance with Section 10.2(b) of this Agreement, the Data Processor shall, taking into account the nature of the processing and the information available to it, assist the Data Controller in notifying the Supervisory Authority of the breach.

This may mean that the data processor must, among other things, help to provide the following information, which according to Article 33(3) of the General Data Protection Regulation must appear in the data controller's notification to the supervisory authority:

- a. The nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data records affected;
- b. Likely consequences of the personal data breach
- c. Measures taken or proposed to address the personal data breach, including, where applicable, measures to limit its potential adverse effects

10 Deletion and return of information

1. **Upon termination of the services relating to processing, the Data Processor is obliged, at the Data Controller's option, to delete or return all personal data to the Data Controller, as well as to delete existing copies, unless EU or national law prescribes the storage of the personal data.**

11 Supervision and audit

- 1. The Processor shall make available to the Controller all information necessary to demonstrate the Processor's compliance with Article 28 of the General Data Protection Regulation and this Agreement and shall enable and contribute to audits, including inspections, by the Controller or another auditor authorised by the Controller.**
2. The detailed procedure for the controller's supervision of the data processor is set out in the Appendix B.
3. The data controller's supervision of any sub-processors is generally carried out through the data processor. The detailed procedure for this is set out in the Appendix B.
4. The Data Processor is obliged to provide authorities who, in accordance with the legislation in force at any given time, have access to the Data Controller's and the Data Processor's facilities, or representatives acting on behalf of the authority, access to the Data Processor's physical facilities against proper identification.

12 Parties' agreements on other matters

1. Any (special) regulation of the consequences of the parties' breach of the data processing agreement will be stated in the parties' "main agreement" or in this agreement's Appendix C.
2. Any regulation of other matters between the parties will be stated in the parties' "main agreement" or in this agreement's Appendix C.

13 Entry into force and termination

1. This Agreement shall enter into force upon signature by both parties.
2. The agreement can be demanded by both parties to be renegotiated if legislative changes or inexpediencies in the agreement give rise to this.
3. Any adjustments/agreements between the parties regarding remuneration, conditions or the like in connection with changes to this agreement will be set out in the parties' "main agreement" or in Appendix D to this agreement.
4. Termination of the data processing agreement can be done in accordance with the terms of termination, including notice period, which appear in the "main agreement".
5. The agreement is valid for as long as the treatment continues. Regardless of the termination of the "Main Agreement" and/or the Data Processing Agreement, the Data Processing Agreement will remain in force until the end of the processing and the deletion of the data by the Data Processor and any sub-processors.
6. Signature

On behalf of the Data Controller

Name:

Position:

Date:

Signature:

On behalf of the data processor

Name: Søren Melgaard

Position: CEO

Date: 04.05.2023

Signature:



14 Contact persons/contact points at the data controller and the data processor

1. The parties can contact each other via the contact persons below:
2. The parties are obliged to inform each other on an ongoing basis of changes regarding the contact person/contact point.

Name:	Søren Melgaard	Name:	
Position:	CEO	Position:	
Telephone number:	+45 82 30 44 40	Telephone number:	
Email:	sme@flealover.com	Email:	

Appendix A: Information about the processing

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

That the data controller can use the system Flea Lover, which is owned and administered by the data processor, to collect and process information about the data controller's members.

The processing of personal data by the Data Processor on behalf of the Data Controller primarily concerns (the nature of the processing):

That the data processor makes the Flea Lover system available to the data controller and thereby stores personal data about the data controller's customers on the sub-processors' servers.

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

Name, e-mail address, telephone number, address, Account information and company registration number.

The processing includes the following categories of data subjects:

Persons who do or have done business with the Data Controller.

The processing of personal data by the Data Processor on behalf of the Data Controller may commence after the entry into force of this Agreement. The duration of the treatment is as follows:

The processing is not limited in time and lasts until the agreement is terminated or terminated by one of the parties.

A.1 Conditions for the data processor's use of sub-processors and list of approved sub-processors

A.2 Conditions for the data processor's use of any sub-processors

The data processor has the data controller's general approval to make use of sub-processors. However, the Data Processor shall notify the Data Controller of any planned changes regarding the addition or replacement of other Data Processors and thereby give the Data Controller the opportunity to object to such changes. Such notification must be received by the data controller at least **1 month** before the use or change is to take effect. If the Data Controller objects to the changes, the Data Controller must notify the Data Processor of this within **1 month** of receipt of the notification. The data controller can only object if the data controller has reasonable, concrete reasons for doing so.

A.3 Approved sub-processors

At the entry into force of the data processing agreement, the data controller has approved the use of the following sub-processors:

Name	Company Reg No.	Address	Description of service
Digital-Ocean, LLC.	VAT ID: EU528002224	101 6th Ave, New York, NY 10013, United States	Hosting/Server Operations
Simply.com A/S	29412006	Højvangen 48660 Skanderborg	Hosting/Server Operations

At the entry into force of the data processing agreement, the data controller has specifically approved the use of the above-mentioned sub-processors for precisely the processing described next to the party. The Data Processor may not – without the Data Controller's specific and written approval – use the individual Sub-Data Processor for a "different" processing as agreed or allow another Sub-Data Processor to carry out the described processing.

Appendix B: Instructions regarding the processing of personal data

A.4 Subject-matter/instructions

The Data Processor's processing of personal data on behalf of the Data Controller takes place by the Data Processor performing the following:

- If the system Flea Lover makes the data controller, in which the data processor stores personal data, and makes backups of this data, available to the data controller - thus the processing is in accordance with the content of the "main agreement".

A.5 Processing safety

The level of security must reflect:

That it is not a matter of processing personal data covered by Article 9 of the General Data Protection Regulation on "special categories of personal data", which is why there is no requirement that a "high" level of security must be established.

- The data processor is then entitled and obliged to make decisions about which technical and organisational security measures are to be used in order to create the necessary (and agreed) level of security around the data.
- However, the Data Processor must – in all cases and as a minimum – implement the following measures agreed with the Data Controller (based on the risk assessment carried out by the Data Controller):
- Access to Flea Lover is through encrypted channels
- User access is through https, with a certificate issued by the Internet Security Research Group (ISRG).
- It can be accessed when the client has knowledge of the username and password. Both parameters are case sensitive.
- Furthermore, https access can be granted via API.
- Data is processed and stored on servers provided by Digital Ocean LLC, with whom there is a data processing agreement. This person is responsible for ensuring the ongoing confidentiality, integrity, availability and robustness of processing systems and services, as well as securing against unauthorized physical/technical access.
- NoviPOS ApS ensures the necessary functionality in relation to traceability in searches for personal data and the data controller's need for anonymization of personal data.

A.6 Storage period/deletion routine

The personal data is stored with the data processor until the data controller requests that the data be deleted or returned.

A.7 Processing site

Processing of the personal data covered by the agreement cannot take place at locations other than the following without the prior written approval of the data controller:

- Gjellerupvej 91a, 8230 Åbyhøj, Denmark. NoviPOS ApS uses the address.
- 101 6th Ave, New York, NY 10013, United States. Digital Ocean LLC uses the address.
- Højvangen 4, 8660 Skanderborg, Denmark. Simply.com uses the address.

A.8 Instructions or approvals regarding the transfer of personal data to third countries

If the Data Controller has not specified in this section or in a subsequent written notification an instruction or approval regarding the transfer of personal data to a third country, the Data Processor may not carry out such a transfer within the framework of the Data Processing Agreement.

A.9 Detailed procedures for the data controller's supervision of the processing carried out by the data processor

The Data Controller may, at its own expense, obtain an audit statement from an independent third party regarding the Data Processor's compliance with this Data Processing Agreement and its appendices.

The data controller's possible expenses in connection with a physical inspection are borne by the data controller himself. However, the Data Processor is obliged to allocate the resources (mainly the time) necessary for the Data Controller to carry out its supervision.

A.10 Detailed procedures for the supervision of the processing carried out by any sub-processors

The Data Processor shall, at the request of the Data Controller, at the expense of the Data Controller, obtain an audit statement from an independent third party regarding the Sub-Processor's compliance with this Data Processing Agreement and its appendices.

In addition, the data processor or a representative of the data processor has access to supervise, including physical supervision, at the sub-processor when, in the opinion of the data processor (or the data controller), a need arises.

Appendix B: Adjustment of other matters by the parties

A.11 Assistance to the Data Controller:

- If the data controller wants assistance in relation to this party's obligation to respond to requests regarding the exercise of the data subjects' rights as stipulated in Chapter 3 of the General Data Protection Regulation, the data processor will provide assistance free of charge for 1 hour. All assistance beyond this first hour will be the responsibility of the data controller.
- If the Data Controller requires information or assistance regarding security measures, documentation or information about how the Data Processor processes Personal Data in general, and such request contains information that goes beyond what is necessary under applicable Data Protection Law, the Data Processor may require payment for such additional services. The Data Processor and its employees must ensure confidentiality in relation to Personal Data processed under the Agreement. This provision shall also apply after termination of the Agreement.