Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

[Organization Name]
[Organization Company Registration Number]
[Organization Address]
[Organization Zipcode and City]
[Organization Country]

(the data controller)

and

NemTilmeld.dk ApS for EasySignup.com
CVR 27 67 31 20
Strømmen 6
DK-9400 Nørresundby
Denmark

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following data processing agreement in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Data Processing Agreement preamble 3
3. The rights and obligations of the data controller 4
4. The data processor acts according to instructions 4
5. Confidentiality 5
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 8
11. Erasure and return of data 9
12. Audit and inspection 9
13. The parties' agreement on other terms 10
14. Commencement and termination 10
15. Data controller and data processor contacts 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

2. Data Processing Agreement preamble

2.1. This data processing agreement set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller. This data processing agreement only governs the processing of personal data that the data processor processes on behalf of the data controller.

2.2. This data processing agreement has 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. The data controller's use of the self-service system EasySignup.com leads to the data processor's processing of personal data on behalf of the data controller in accordance with this data processing agreement.

2.4. The self-service system EasySignup.com is a web based standard system used to administrate the data controller's events. In the self-service system the events are managed through an administration area on the data controller's access protected account at the data processor. The data processor's processing of personal data on behalf of the data controller is on a fundamental basis done automatically by the self-service system based on the way the data controller's users use and set up the features in the administration area on the account in the self-service system. Access to the administration area on the account in the self-service system is given by the data controller through a username for the account. Each username can be granted different rights. Access to use and set the features in the administration area of the self-service system therefore depends on the rights that are given to each individual username on the account. The persons that the data controller has given an username to the administration area of the self-service system is in the following referred to as "the data controller's users".

2.5. The conditions for subscribing to the web based self-service system EasySignup.com are regulated in the "Terms of Use - subscription to EasySignup.com" (in the following referred to as "terms of use")

2.6. This data processing agreement and the "terms of use" shall be interdependent and cannot be terminated separately. The data processing agreement may however - without termination of the terms of use - be replaced by an alternative valid data processing agreement.

2.7. This data processing agreement shall take priority over any similar provisions contained in other agreements between the parties, including the terms of use.

2.8. Three appendices are attached to this data processing agreement and form an integral part of this data processing agreement.

2.9. 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.

2.10. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and reference to a list of sub-processors authorised by the data controller.

2.11. Appendix C contains the data controllers 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.

2.12. This data processing agreement along with appendices shall be retained in writing, including electronically, by both parties.

2.13. This data processing agreement shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (in the following referred to as 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 EU and EEA Member States (in the following referred to as "Member States") data protection provisions and this data processing agreement.

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.

3.4. The self-service system automatically creates a set of "terms of registration" based on how the controller's users use and set up the features in the administration area of the self-service system. The terms of registration governs the relationship between the data controller and the guests who sign up for the data controller's events (in the following referred to as attendees) and must be approved by the attendees before they can sign up for the data controller's events. The data controller's users are obligated to read and verify whether the information in the terms of registration is adequate in relation to the compliance of the GDPR and applicable EU or Member States data protection provisions before the self-service system can be used for an event. The self-service system asks the data controller's users to approve each set of terms of registration before the terms can be used.

3.5. The data controller has the full responsibility for the data controller's users use and settings of the features in the administration area of the self-service system are in accordance with the GDPR, applicable EU or Member State data protection provisions and this data processing agreement.

3.6. The data controller has the full responsibility for managing user rights and user access to the data controller's account in the self-service system, including assessing and addressing any issues that may arise in sharing login details.

3.7. The data controller must inform the data controller's users of the obligations that lie with each user under this data processing agreement and the terms of use.

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 given up front, documented and kept in writing, including electronically, in connection with this data processing agreement.

4.2. If it comes to the data processor's attention, 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.

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 and consequences to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks and consequences. 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 and consequences to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks and consequences.

The assessment of the risks and consequences to the rights and freedoms of natural persons which are in the data processor's self-service system is conducted by the data processor on an overall level, based on the general use of the self-service system. The assessment is therefore not based on individual circumstances of the data controller. The data processor's overall assessment of the security level can be found in Appendix C.2.

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

The data controller must assess whether or not the measures taken by the data processor are adequate in relation to the data controller's identified risks and consequences of the data subject's when using the data processor's standard self-service system. The security level of the processing is described in more details in Appendix C.2 together with the measures the data processor as a minimum must implement. If the data controller's identified risks and consequences of the data subject's require additional measures, the data processor would like to discuss the possibility of implementing the measures if they match the overall assessment of the risks and consequences to the rights of natural persons and thus benefit all the data processor's customers.

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 this data processing agreement 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 40 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). If the data controller should object to the changes, the data controller shall notify the data processor of this within 20 days of receipt of the notification. The data controller shall only object if the data controller has reasonable and specific grounds for such refusal. The list of sub-processors already authorised by the data controller is referred to 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 this data processing agreement 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 this data processing agreement 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 this data processing agreement 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 this data processing agreement is 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 this data processing agreement:

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 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. This data processing agreement shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and this data processing agreement 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, 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, 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 this data processing agreement 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 must be made by the data processor by giving a preliminary notification within 4 hours after the data processor has discovered the breach and a more detailed notification within 36 hours after the data processor has discovered the 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 this data processing agreement 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 delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

11.2. The following EU or Member State law applicable to the data processor requires storage of the personal data after the termination of the provision of personal data processing services:

a. The Danish Bookkeeping Act after which payment information must be stored for the remainder of the relevant financial year and additional 5 years.

11.3. The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions. Storage periods and erasure procedures are described in more details in Appendix C.

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 this data processing agreement 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. Any liability under or according to this data processing agreement is governed by the liability clauses in the terms of use.

13.2. The level of any compensation to the data processor under or according to this data processing agreement is governed by the terms of use.

13.3. Regulation of jurisdiction and venue is specified in the terms of use and applies to this data processing agreement.

14. Commencement and termination

14.1. This data processing agreement becomes effective on the date where both parties has accepted it. Either by signature or checking a separate check box in the self-service system. This data processing agreement replaces any previous data processing agreements with EasySignup.com.

14.2. Both parties shall be entitled to require this data processing agreement renegotiated if changes to the law or inexpediency of this data processing agreement should give rise to such renegotiation. The other party must be reached and notified of any changes at least 30 days prior to the changes taking effect.

14.3. This data processing agreements shall apply as long as the data processor stores personal data processed on behalf of the data controller. This data processing agreement and the terms of use can therefore not be terminated during this period. The services referred to in item 11.1 terminates, when the dataprocessor has deleted all personal data stored on behalf of the data controller. The personal data is deleted as described in Appendix C.4.

14.4. Signature

On behalf of the Data Controller	On behalf of the Data Processor	
	Name:	Thomas Kjærgaard
	Position:	Customer helper and founder
	Date:	[Date of document being sent for signature]
	Signature:	[Inserted signature]

15. Data controller and data processor contacts

15.1. The parties may contact each other using the following contacts.
The data processor will consider this contact person at the data controller as the one responsible for the use of the self-service system EasySignup.com (system responsible). It is therefore this contact person that the data processor will contact regarding matters in this data processing agreement e.g. in case of any data breach.

Contact person at the data controller (system responsible):		Contact person at the data processor:	
Name:	[Stated name]	Name:	Thomas Kjærgaard
Position:	[Stated position]	Position:	Customer helper and founder
Telephone number:	[Stated telephone number]	Telephone number:	+45 70404061
E-mail:	[Stated e-mail]	E-mail:	thomas@EasySignup.com

15.2. Contact information of the data protection officer (DPO) or person responsible for data protection at the data controller.

Name:	[Stated name]
Position:	[Stated position]
Telephone number:	[Stated telephone number]
E-mail:	[Stated e-mail]

The contact information will appear in the terms of registration that governs the data controller's relationship with the attendees. The terms of registration can be found on the public website where the attendees sign up for the controller's event. The contact information will be specified as the information the attendees should use when the attendees wish to exercise their rights under the GDPR.

15.3. The parties are obligated to inform each other of changes in the contact information. The data controller's users who have access to the self-service system as an administrator can change the contact information in the administration area of the self-service system. If the contact information is changed in the self-service system, the data processor will use the latest updated contact information.

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 that the data controller can use the web based self-service system EasySignup.com for the administration of the data controller's events. The self-service system EasySignup.com helps the data controller to collect and manage many of the tasks connected to the administration of an event, including managing the sign up process and overview of the attendees already signed up for the event.

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

The data processor deliver the web based self-service system EasySignup.com to the data controller for the administration of the data controller's events. Through the self-service system the data processor therefore collects and stores personal data on behalf of the data controller.

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

General personal data:

- The standard configuration of the self-service system is that only general personal data is processed, such as: name, email address, telephone number, company/organization and job title.
- If payment is required to attend an event through the self-service system, the self-service system requires the following general personal data: name, email address and address:
    - For payment by debit card: The data processor uses payment services to verify and acquire the transaction and does therefore not store card number, account number, CVC etc. in the self-service system. The data processor has access to information about the card type, issuing country and a censored version of the card number, meaning the last four digits of the card number.
    - For payment using the Danish invoice paymentsystem (FI payment (Fælles Indbetalingssystem)): To refund a canceled registration where payment was made by an invoice through a FI payment the money must be refunded to the attendee by a bank transfer to an account number. The data processor therefore records and stores an account number for such a refund.

Special categories of personal data (including criminal convictions and offences)

- The data controller's organization, company or the type of event held e.g. a political event may cause an event to contain special categories of personal data (including criminal matters) solely because the attendees are participating, and thus may be assumed to be involved in what the event is about e.g. policy, events for patients, etc.
- Through the administration area in the self-service system, the data controller's users manage the data controller's events by creating and editing each event. When creating and editing an event in the administration area, the data controller's users determine, among other things, what information each attendee must provide in order to sign up for an event. Therefore, the data controller's users can use and set the features in the administration area of the self-service system in a manner that allows special categories of personal data to be processed (including criminal matters). An example is if the data controller's users ask if an attendee has an allergy.

When the data controller's users use and set the features in the administration area of the self-service system the self-service system automatically does what the data controller's users specify, and therefore does not restrict the data controller's users in setting up the events. Neither in the type of the event nor in relation to what personal data the data controller's users collect about the attendees, e.g. whether the attendee has an allergy. The data controller's users are therefore able to obtain all types of personal data through the self-service system and how the data controller's users use and set the features in the administration area of the self-service system can therefore lead to further processing of general personal data, special categories of personal data and criminal data.

The data processor does not process additional general personal data, special categories of personal data or personal data on criminal matters unless the data controller's users instruct the data processor to do so through the use or setting of the features in the administration area of the self-service system.

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

- Potential attendees who visit the website for signing up for an event
- Persons invited to the data controller's events
- Upcoming and past attendees for the data controller's events
- The data controller's contacts
- The data controller's users, who are the persons who through a username manage the data controller's events in the administration area on the data controller's account in the self-service system.

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

The processing is not time-limited and is performed until the data processor no longer stores the personal data being processed on behalf of the data controller. A description of the storage periods and erasure procedures is provided in Appendix C.4 of this data processing agreement.

Appendix B

Authorised sub-processors

B.1. Approved sub-processors

The data processor's sub-processors is listed on the website https://www.EasySignup.com/conditions/subprocessors/. On commence of this data processing agreement the data processor does not use any sub-processors as stated in the list of sub-processors version 1 on the website.

The list of sub-processors is placed on the website https://www.EasySignup.com/conditions/subprocessors/ in order for the data processor to adjust the self-service system and maintain the flexibility in the development of the self-service system, if the development makes it necessary to use a sub-processor or subsequently change the activity of the processing made by a sub-processor.

The data processor shall not be entitled to engage a sub-processor or subsequently change the activity of the processing made by a sub-processor without the data controller's prior explicit written authorisation or upon timely notification to the data controller pursuant to Clause 7.3 of this data processing agreement, where the data controller has not objected.

The current version of the list of sub-processors, which the data controller has either approved or timely been notified without objections, can bee found in the administration area on the data controller's account in the self-service system.

Appendix C

Instruction pertaining to the use of personal data

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

The data processor processes personal data on behalf of the data controller when the data processor deliver the web based self-service system EasySignup.com to administrate the data controller's events. The processing of personal data on behalf of the data controller will be in accordance with the terms of use and this data processing agreement.

The web based self-service system automatically does what the data controller's users specify when using and setting the features in the administration area of the self-services system. The data processor's processing on behalf of the data controller is therefore continuously influenced by how the data controller's users use and set the features in the administration area of the self-service system.

If it is necessary in order to deliver the web based self-service system EasySignup.com for the administration of the data controller's events, the data processor can, in addition to the sub-processors described in Appendix B.1. pass on selected personal data to external partners, such as payment service providers and a telephone service provider.

Personal data is only disclosed to an external partner if it is necessary based on the use of the self-service system. The personal data disclosed to an external partner is limited to the personal data necessary for the external partner to deliver the desired function, such as:

- If an attendee calls the data processor, a telephone number will be disclosed to the data processor's telephone provider for the data processor to answer the call from the attendee.
- If the data controller communicates with the attendees by sending an SMS text message through the self-service system, a telephone number and the content of the SMS text message will be disclosed to the data processor's telephone provider in order for the data processor to send the SMS text message to the attendees.
- If payment is required to attend an event through the self-service system and payment is made by debit card, this information is disclosed to the data processor's payment service providers, respectively a payment gateway end payment acquirers: a payment ID, amount and the currency in which the amount is to be paid. Card number, expiry date, CVC etc. is not disclosed by the data processor but entered directly by the attendee in the payment gateway provider's system when completing the card payment.
  If the data processor through the payment acquirers receives an objection to the card payment made in the self-service system by the attendee, the data processor will disclose information about which event the attendee has purchased and the name of the organizer to the payment acquirers in order to refute the objection. This disclosure is necessary because it is the data processor's agreements with the acquirer that are used for the card payments.
- If an invoice with an FI payment is cancelled and the payment therefore must be refunded, this information is disclosed to the data processor's bank, so the data processor can refund the payment: a credit note number, an original invoice number, a payment number, an amount, the currency in which the amount must be refunded, an account number, the first name and last name of the attendee.

Upon termination of the subscription, the data processor must store the personal data on the data controller's account, in accordance to the storage and deletion settings, sepcified by the data controller in the self-service system. When the specified storage period ends, the personal data is deleted automatically. During the storage period, the data controller will not have access to the personal data, unless the subscription is renewed. When there is a need, the data controller can contact the data processor, who will assist the data controller with the compliance of the data subject's rights.

C.2. Security of processing

The level of security shall take into account:

That the data processor generally processes a large volume of personal data on behalf of many different data controllers. As a standard configuration of the self-service system it only processes general personal data. However, individual users use and settings of the features in the administration area of the self-service system can cause that personal data covered by Article 9 of the GDPR on "special categories of personal data" and Article 10 of the GDPR on "personal data on criminal offenses" is being processed. The data processor therefore operates at a relatively high level of security because the self-service system is used by many different data controllers.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organizational 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 self-service system is designed to be robust and technically resistant.
- Backup and recovery procedures haves been established.
- All access to IT-systems, servers and PC's containing confidential information, personal data and critical data is restricted based on specific authorizations. Access will only be authorized to persons for whom access is necessary in order to carry out audit or operational and technical tasks.
- Once a year access rights are reviewed, to secure that employees are authorized the necessary access rights.
- All electronic accesses require a personal user ID and password.
- Personal data is effectively and securely erased when disposing IT equipment.
- None of attendees' personal data is stored in printed form. Employees do not print attendees' information from the system unless separate instructions have been given by the data controller. This could be in connection with support regarding name tags.
- Access to the data processor's own physical servers is secured with lock and alarm. Only the employees for whom access is necessary, have access to the room(s) in question.
- All transfer of personal data in the self-service system is carried out through encrypted connections.
- Only specifically authorized employees have remote access to the data processor's internal network, and this always takes place through encrypted VPN connections.
- The self-service system logs all users' access and activity in the system in order to establish who has requested and viewed information, requested payments etc. in the event that an investigation hereof becomes necessary.
- Keywords logged, when users perform searches in the administration area of the self-service system, may contain personal data about attendees. Keywords that are logged, will be deleted 6 months after a search has been made.
- Rejected or failed login attempts to the self-service system are monitored and automatically logged. If more than 5 continuous failed login attempts are logged, a time delay is installed between subsequent possible login attempts.

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:

- "Privacy by design" based on the overall level of security described in Appendix C.2. is a focus in the data processor's development of the standard self-service system for administrating events.
- In the development of the standard self-service system the data processor focuses on giving the data controller's users the opportunity to respect the rights of the data subjects when setting up events through the various features in the administration area of the self-service system.
- Features related to the processing of personal data in the self-service system is described by the processor in the guide "How to manage personal data in EasySignup" at the website: https://www.EasySignup.com/support/guides/83/gdpr-general/. The website will constantly be updated and possibly changed as the data processor develops features in the self-service system.
- The data processor does not respond to or resolve a request from an attendee to the data controller's events on their rights, including insights, but passes the query on to the data controller as soon as the data processor is aware that the data controller is the one that must process the request.
- In the event of a data breach, the data processor will assist the data controller, with all the information available to the data processor, in order for the data controller to both assess the extent of the breach, report the breach to the supervisory authority and notify the data subject.
- The data processor is entitled to be compensated for its employees' time used on assistance to the data controller which is not a basic need or requirement for the majority of the data controllers using the self-service system. This means that:
    - The data processor is entitled to be compensated for its employee's time used on assisting the data controller with the reporting of a breach to a supervisory authority and the notification of the breach to the data subject, unless the breach is due to the data processor. This is assistance according to 9.2.a and 9.2.b of this data processing agreement.
    - The data processor is entitled to be compensated for its employee's time used on assisting the data controller to carry out a data protection impact assessment and assistance to the data controller's consulting with the supervisory authority depending on the result of the data protection impact assessment. This is assistance according to 9.2.c and 9.2.d of this data processing agreement.

C.4. Storage period/erasure procedures

According to the standard setting in the self-service system personal data is automatically erased from the system according to the periods described below:

- When the payment module is in use: Payment information is stored for the remainder of the relevant financial year and an additional 5 years. All other personal data is erased 2 years after the event has ended.
- When the payment module is not in use: Personal data is stored for 2 years after the event has ended.

The data controller's users can at any time change the settings using the features in the administration area of the self-service system. The data controller's users can therefore delete personal data and choose how long it will take before the system automatically deletes personal data. Only exception is personal data that is required by the Danish Bookkeeping Act, this information can be set to be deleted at the earliest 5 years after the end of the financial year to which the material relates or later.

It is the data controller who, through features in the self-service system, choose how long the personal data in the self-service system is stored and when the system deletes personal data. The data processor follows the storage and deletion settings specified on the data controller's account in the self-service system. If the data controller does not change the storage and deletion settings on the data controller's account in the self-service system, the personal data will be deleted according to the standard settings.

Before the termination of the subscription and before the access to the self-service system is closed, the data controller can delete personal data through features in the self-service system. Personal data that is required by the Danish Bookkeeping Act, can at the earliest be deleted 5 years after the end of the financial year to which the material relates.

If the data controller has not deleted personal data before the access to the self-service system is closed, the data processor is instructed to store personal data in accordance with the storage and deletion settings, specified by the data controller in the self-service system. When the specified storage period ends, the personal data is deleted automatically. During the storage period, the data controller will not have access to the personal data unless the subscription is renewed. When there is a need, the data controller can contact the data processor, who will assist the data controller with the compliance of the data subject's rights.

C.5. Processing location

The data processor's servers and offices are located at the following locations in Denmark:

Strømmen 6
9400 Nørresundby
Denmark

and

Ankeret 7
9200 Aalborg Øst
Denmark

In order to respond quickly and adjust the self-service system to maintain a robust and resistant self-service system, the data processor can move to or place servers and offices at other locations in Denmark without prior written approval by the data controller. The data processor will inform the system responsible at the data controller of any changes in the locations. The data processor cannot move to or place servers at locations outside Denmark without a prior written consent from the data controller

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

If the data controller does not in this data processing agreement 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 this data processing agreement 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 at the data processor's expense obtain an audit report ISAE 3000 from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and this data processing agreement. Upon request, the latest version of the ISAE3000 audit report will be made available to the data controller.

Based on the results of such an audit report, 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 this data processing agreement. The request for additional measures will be implemented if they fit into the data processor's overall delivery of a standard self-service system used to administrate events and therefore will benefit all of the data processor's customers. Whether further measures are implemented is therefore assessed by the data processor based on the overall assessment of the risks and consequences to the rights of individuals, as described in Clause 6.2 of this data processing agreement.

The data controller or the data controller's representative shall by further agreement in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

When disregarding the audit report ISAE 3000 the data processor is entitled to be compensated for its employees' time used in relation to supervision, audit or inspection visit initiated by the data controller, unless it is requested by the supervisory authority due to an inability by the data processor to comply with GDPR, the applicable EU or Member States data protection provisions.

The data controller shall be entitled to obtain once every year at the data controller's expense an inspection report from an independent third party with regards to the data processor's compliance with the treatment of personal data.

Inspections and audits from others than those appointed by the data processor and which will give access to business secrets and technical details of the data processors setup must obtain a security clearance by the data-processor or a third party used by the data-processor for security-clearances before the inspection or audit can be conducted.

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

The data processor shall once a year at the data processor's expense carry out an inspection, including physically inspect, concerning the sub-processor's compliance with this data processing agreement.

The data processor or the data processor's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data processor (or the data controller) deems it required.

Documentation for such inspections of the sub-processors shall upon request be sent to the data controller.

The data controller may - if required - elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to this data processing agreement.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and this data processing agreement.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor and the sub-processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

The data processor is entitled to be compensated for its employees' time used in relation to the supervision, audit or inspection visit of the sub-processor initiated by the data controller, unless it is requested by the supervisory authority due to an inability by the data processor to comply with the GDPR and the applicable EU or Member State data protection provisions.

Any expenses incurred by the sub-processor for inspection and audit of the sub-processor initiated by the data controller are defrayed by the data controller.

Before an inspection or audit can be conducted at the sub-processor, the sub-processor has the right to require security clearance from persons who conduct an inspection or audit of the sub-processor if the inspection or audit gives them access to business secrets and technical details of the sub-processors setup.