Data processing agreement

Between

Name
CVR
Address
ZIP code and town
Country
(The Data Controller)

and

3dsecure.io ApS
CVR 41019328
P.O. Pedersensvej 14
8200 Aarhus N
Denmark
(The Data Processor)

Content

1. Data Processing Agreement preamble 3

2. The rights and obligations of the Data Controller 4

3. The data processor acts according to instructions 4

4. Confidentiality 5

5. Security of processing 5

6. Use of Sub-Processors 6

7. Transfer of data to third countries or international organizations 7

8. Assistance to the data controller 7

9. Notification of personal data breach 9

10. Erasure and return of data 9

11. Inspection and audit 10

12. Contact persons 10

Appendix A: Information about the processing 11

Appendix B: Terms of the Data Processor's use of sub-processors and list of approved sub-processors 12

Appendix C: Instructions pertaining to the use of personal data 14

1. Data Processing Agreement preamble

1. This Data Processing Agreement sets out the rights and obligations that apply to the Data Processor's handling of personal data on behalf of the Data Controller.

2. This Agreement has been designed to ensure the Parties' compliance with Article 28, sub-section 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 data processing agreement.

3. The Data Processor's processing of personal data shall take place for the purpose of fulfilment of the Parties' "main agreement".

4. The Data Processing Agreement and the "Main Agreement" shall be interdependent and cannot be terminated separately. The Data Processing Agreement may, however - without termination of the "main agreement" - be replaced by an alternative valid data processing agreement.

5. The Data Processing Agreement shall take precedence over any similar provisions contained in other agreements between the Parties, including the "Main Agreement".

6. Three appendices are attached to this Data Processing Agreement. The Appendices form an integral part of this Data Processing Agreement.

7. Appendix A of the Data Processing Agreement contains details about the processing as well as the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

8. Appendix B of the Data Processing Agreement contains the Data Controller's terms and conditions that apply to the Data Processor's use of Sub-Processors and a list of Sub-Processors approved by the Data Controller.

9. Appendix C of the Data Processing Agreement contains instructions on the processing that the Data Processor is to perform on behalf of the Data Controller

(the subject of the processing), the minimum security measures that are to be implemented and how inspection with the Data Processor and any Sub-Processors is to be performed.

10. The Data Processing Agreement and its associated Appendices shall be retained in writing as well as electronically by both Parties.

11. 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 or other legislation.

2. The rights and obligations of the Data Controller

1. The Data Controller shall be 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 Danish Data Protection Act.

2. The Data Controller shall be responsible for ensuring that the processing that the Data Processor is instructed to perform is authorised by law.

3. The data processor acts according to instructions

1. The Data Processor shall solely be permitted to process personal data on documented instructions from the Data Controller unless processing is required under EU or Member State law to which the Data Processor is subject; in this case, the Data Processor shall inform the Data Controller of this legal requirement prior to processing, unless that law prohibits such information on important grounds of public interest cf. Article 28. Sub-section 3, para a.

2. The Data Processor shall immediately inform the Data Controller if instruction in the opinion of the Data Processor contravenes the General Data Protection Regulation or data protection provisions contained in other EU or Member State law.

4. Confidentiality

1. The Data Processor shall ensure that only those persons who are currently authorized to do so are able to access the personal data being processed on behalf of the Data Controller. Access to the data shall therefore without delay de denied if such authorisation is removed or expires.

2. Only persons who require access to the personal data in order to fulfil the obligations of the Data Processor to the Data Controller shall be provided with authorisation.

3. The Data Processor shall ensure that the persons authorized to process personal data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to a suitable statutory obligation of confidentiality.

4. The Data Processor shall at the request of the Data Controller, be able to demonstrate that the employees concerned are subject to the above confidentiality.

5. Security of processing

1. The Data Processor shall take all measures required under Article 32 of the General Data Protection Regulation, which stipulates that with consideration for the current level, implementation costs, the nature, scope, context and purpose of the processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2. The above obligation entails that the Data Processor shall perform a risk assessment and thereafter implement measures to counter the identified risk. Depending on their relevance, the measures may include the following:
    a. Pseudonymization 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 regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

3. The Data Processor shall in ensuring the above - in all cases - at a minimum, implement the level of security and the measures specified in Appendix C to this Data Processing Agreement.

6. Use of Sub-Processors

1. The Data Processor shall meet the requirements specified in Article 28, sub-section 2 and 4, of the General Data Protection Regulation in order to engage another processor (Sub-Processor).

2. The Data Processor shall therefore not engage another processor (Sub-Processor) for the fulfilment of the Data Processing Agreement without the prior specific or general written approval from the Data Controller.

3. In the event of general written consent, the Data Processor shall inform the Data Controller of any planned changes regarding additions to or replacement of other data processors and thereby give the Data Controller the opportunity to object to such changes.

4. The Data Controller's requirements for the Data Processor's engagement of other sub-processors shall be specified in Appendix B to this Data Processing Agreement.

5. The Data Controller's consent to the engagement of specific sub-processors, if applicable, shall be specified in Appendix B to this Data Processing Agreement.

6. When the Data Processor has the Data Controller's authorisation to use a sub-processor, the Data Processor shall ensure that the Sub-Processor is subject to the same data protection obligations as those specified in this Data Processing Agreement on the basis of a contract or other legal document under EU law or the national law of the Member States, in particular providing the necessary guarantees that the Sub-Processor will implement the appropriate technical and organisational

measures in such a way that the processing meets the requirements of the General Data Protection Regulation.

7. Transfer of data to third countries or international organizations

1. The Data Processor shall only be permitted to process personal data on documented instructions from the Data Controller, including transfer (assignment, disclosure and internal use) of personal data to third countries or international organisations, unless processing is required under EU or Member State law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless law prohibits such information on important grounds of public interest, cf. Article 28, sub-section 3, para a.

2. Without the instruction or approval of the Data Controller, the Data Processor therefore cannot - within the framework of this Data Processing Agreement;
    a. disclose personal data to a data controller in a third country or in an international organization,
    b. assign the processing of personal data to a sub-processor in a third country,
    c. have the data processed in another of the Data Processors's divisions which are located in a third country.

3. The Data Controller's instructions or approval for the transfer of personal data to a third country shall be set out in Appendix C to this Data Processing Agreement.

8. Assistance to the Data Controller

1. The Data Processor, taking into account the nature of the processing, shall, as far as possible, assist the Data Controller with the appropriate technical and organisational measures, in the fulfilment of the Data Controller's obligations to respond to requests for the exercise of the data subjects' right pursuant to Chapter 3 of the General Data Protection Regulation.

    This entail that the Data Processor should as far as possible assist the Data Controller in the Data Controller's compliance with:
    a. notification obligation when collecting personal data from the data subject
    b. notification obligation if personal data have not been obtained from the data subject

c. 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 restrict 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 to object to the result of automated individual decision-making, including profiling

2. The data processor shall assist the Data Controller to ensure 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 data made available to the Data Processor, cf. Article 28, sub-section 3 para f.

   This entails the Data Processor should take into account the nature of the processing, as far as possible, when assisting the Data Controller in the Data Controller's compliance with:

   a. the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing
   b. the obligation to report personal data breaches to the supervisory authority (Danish Data Protection Agency) without undue delay and, if possible, within 72 hours of the Data Controller discovering such breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons
   c. the obligation – without undue delay - to communicate the personal data breach to the data subject when such breach is likely to result in a high risk to the rights and freedoms of natural persons
   d. the obligation to carry out a data protection impact assessment if a type of processing is likely to result in a high risk to the rights and freedoms of natural persons
   e. the obligation to consult with the supervisory authority (Danish Data Protection Agency) prior to processing if a data protection impact

assessment shows that the processing will lead to high risk in the lack of measures taken by the Data Controller to limit risk.

9. Notification of personal data breach

1. On discovery of personal data breach at the Data Processor's facilities or a sub-processor's facilities, the Data Processor shall without undue delay notify the Data Controller.
   The Data Processor's notification to the Data Controller shall, if possible, take place within 48 hours after the Data Processor has discovered the breach to enable the Data Controller to comply with his obligation, if applicable, to report the breach to the supervisory authority within 72 hours.

2. According to Clause 9.2., para b, of this Data Processing Agreement, the Data Processor shall - taking into account the nature of the processing and the data available - assist the Data Controller in the reporting of the breach to the supervisory authority.
   This can mean that the Data Processor is required to assist in obtaining the information listed below, which, pursuant to Article 33, sub-section 3, of the General Data Protection Regulation, shall be stated in the Data Controller's report to the supervisory authority:
   a. The nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects and the categories and the approximate number of affected personal data records
   b. Probable consequences of a personal data breach
   c. Measures which have been taken or are proposed to manage the personal data breach, including, if applicable, measures to limit its possible damage

10. Erasure and return of data

1. On termination of the processing services, the Data Processor shall be under obligation, at the Data Controller's discretion, to erase or return all the personal data to the Data Controller and to erase existing copies unless EU or national law requires storage of the personal data.

11. Inspection and audit

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and this Data Processing Agreement, and allow for and contribute to audits, including inspections performed by the Data Controller or another mandated by the Data Controller.

2. The procedures applicable to the Data Controller's inspection of the Data Processor are specified in Appendix C to this Data Processing Agreement.

3. The Data Controller's inspection of any sub-processors, if applicable, shall, as a rule, be performed through the Data Processor. The procedures for such inspection are specified in Appendix C to this Data Processing Agreement.

4. 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.

12. Contact persons

David Andersen - Full Stack Developer - da@clearhaus.com
Søren Soltveit - CTO - ss@clearhaus.com

Appendix A: Information about the processing

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

- To receive and process information for the purpose of securing authentication of payers by card payments online.

The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

- That the Data Processor collects information which is sent to Visa and Mastercard, which subsequently provides via the Data Processor whether the cardholder in the transaction in question can be authenticated.

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

- Name, email address, phone number, address, payment information, browser information and IP address

Processing includes the following categories of data subjects:

- People who hold a debit card and make a payment through a system using the data processor's service.

Appendix B: Terms of the Data Processor's use of sub-processors and list of approved sub-processors

Terms for the Data Processor's use of any sub-processors

The Data Processor has the general authorization of the Data Controller 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, thereby allowing the Data Controller to object to such changes. Such notification must reach the Data Controller at least 1 month before the application or change is to take effect. If the Data Controller objects to the changes, the Data Controller must notify the Data Processor within 5 working days from the notification. The Data Controller can only object if the Data Controller has reasonable or concrete reasons for this.

Approved sub-processors

The Data Controller shall on commencement of this Data Processing Agreement approve the engagement of the following sub-processors:

Name	CVR-no.	Address	Description of processing
Amazon Web Services EMEA SARL	B 186.284	38 avenue John F. Kennedy, L-1855 Luxembourg Luxembourg	Technical infrastructure, where the software is run and data is stored.
Visa Europe Limited	Z8657396	1 Sheldon Square London, W2 6TT England	All collected data
Mastercard Inc.	0448.038.446	Chaussée de Tervuren 198A 1410 Waterloo Belgium	All collected data
Issuing banks (ACS) - non-dependent on the specific bank			

The Data Controller shall on the commencement of this Data Processing Agreement specifically approve the use of the above sub-processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's explicit written consent – to engage a sub-processor for 'different' processing than the one that has been agreed or have another sub-processor perform the described processing.

Appendix C: Instructions pertaining to the use of personal data

The subject of/instruction of the processing

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:

- The Data Processor receives data to verify the cardholder's access to debit cards. The information is sent to the card organizations as well as the issuing bank that performs the actual verification.

Security of processing

The level of security shall reflect:

- The fact that a large amount of personal data is covered by Article 9 of the General Data Protection Regulation on "special categories of personal data", therefore a high level of security must be established.
- The Data Processor is then obliged to make decisions about the technical and organizational security measures to be used to create the necessary and agreed level of security around the information.
- The Data Processor shall, however - in the event and at a minimum - implement the following measures that have been agreed with the Data Controller (based on the risk assessment carried out by the Data Controller):
- That the system is subject to the PCI DSS and PCI 3DS security standards.
- That information such as the cardholder's name and address is stored anonymously in the system and data is encrypted to relevant parties.

Storage period

The personal data is stored for a maximum of 5 years, after which it is deleted from the data processor.

Processing location

Processing of the personal data under this Data Processing Agreement cannot be performed at other locations than the following without the Data Controller’s prior written consent:

- AWS eu-west-1, Ireland

Instruction for or approval of the transfer of personal data to third countries

In principle, data will only be transferred to third countries if the card used is issued in a third country.

Procedures for the Data Controller's inspection of the processing being performed at the Data Processor

The Data Processor, at the request of the Data Controller, shall, on behalf of the Data Controller, obtain a Statement of Assurance from an independent third party regarding the Data Processor's compliance with this Data Processing Agreement and its appendixes. Internal time spent by the Data Processor will be billed at EUR 300.00 per hour.
The Statement of Assurance is sent as soon as possible after obtaining the information to the Controller.
In addition, the Data Controller or a representative of the Data Controller has the right to inspect, including physical supervision, at the Data Processor, when there is a need to do so, in the opinion of the Data Controller. Internal time spent by the data processor will be billed at EUR 300.00 per hour.