Data Processing Agreement

for

the Data Processor

Logos Payment Solutions A/S

CVR No. 26393647

Nærum Hovedgade 6

2850 Nærum

Denmark

January 2021

1 Table of Contents

2 Background for the Data Processing Agreement 3

3 Rights and Obligations of the Data Controller 3

4 The Data Processor Acts As Instructed 4

5 Confidentiality 4

6 Security of Processing 4

7 Use of Sub-Processors 5

8 Transfer of Data to Third Countries or International Organisations 5

9 Assistance to the Data Controller 5

10 Notification of Breach of Personal Data Security 7

11 Erasure and Return of Data 7

12 Supervision and Audit 7

13 Duration and Termination 8

Appendix A Information on Processing 9

Appendix B Terms and Conditions for the Use of Sub-Processors by the Data Processor 10

Appendix C Instructions Concerning the Processing of Personal Data 11

2 Background for the Data Processing Agreement

1. This Agreement lays down the applicable rights and obligations when the Data Processor processes personal data on the Data Controller's behalf.

2. The Agreement has been formulated with an eye to compliance by the parties with Article 28, para. 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 (the General Data Protection Regulation)*, which places specific requirements on the contents of data processing agreements.

3. This Data Processing Agreement shall take precedence to any corresponding provisions in other agreements signed between the parties.

4. The three appendices enclosed herewith belong to and shall be considered an integral part of this Agreement.

5. Appendix A to the Data Processing Agreement contains detailed information on the processing, including on the purpose and nature of the processing, the type of personal data, categories of data subjects and duration of processing.

6. Appendix B to the Data Processing Agreement contains a list of possible sub-processors that are used.

7. Appendix C to the Data Processing Agreement contains detailed information on the type of processing the Data Processor undertakes on the Data Controller's behalf (the subject-matter of the processing), the safety measures that are observed and how the Data Processor and any sub-processors are supervised.

8. Copies of the Data Processing Agreement with appendices shall be kept by both parties.

9. This Data Processing Agreement does not release the Data Processor from obligations that are imposed on the Data Processor by virtue of the General Data Protection Regulation or any other legislation.

3 Rights and Obligations of the Data Controller

1. As a general rule, the Data Controller is responsible to the general public (including to 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. Thus, the Data Controller has both the rights and obligations to make decisions on the purposes of and means for the processing.

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 perform.

4 The Data Processor Acts As Instructed

1. Unless required to do so by Union or Member State law to which the Data Processor is subject, the Data Processor must only process personal data subject to documented instructions from the Data Controller. In this case, the Data Processor informs the Data Controller of this legal requirement prior to processing, unless that law prohibits such disclosure on important grounds of public interest, cf. Article 28(3)(a).

2. The Data Processor notifies the Data Controller immediately if an instruction infringes, in the Data Processor's opinion, on the General Data Protection Regulation or data protection provisions of another Union law or the national law of Member States.

5 Confidentiality

1. The Data Processor ensures that only personnel authorised for this have access to the personal data that are processed on the Data Controller's behalf. Access to information shall therefore be denied immediately if the authorisation is withdrawn or expires.

2. The Data Processor shall ensure that personnel who are authorised to process personal data on the Data Controller's behalf have pledged to observe confidentiality or are subject to an appropriate statutory confidentiality obligation.

6 Security of Processing

1. Taking into account the current level, cost of implementation, and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller shall implement all appropriate technical and organisational measures as are required pursuant to Article 32 of the General Data Protection Regulation for ensuring a level of security that addresses these risks.

2. In connection with the above, the Data Processor shall — in all cases — as a minimum, implement the security level and the measures specified in detail in Appendix C to this Agreement.

3. If the Data Controller subsequently places requirements for additional security measures on the Data Processor, these shall be established at the Data Controller's expense and subject to the sales and delivery terms and hourly rates of the Data Processor that are applicable at any time.

7 Use of Sub-Processors

1. To use another data processor (a sub-processor), the Data Processor shall meet the conditions provided for in Article 28(2) and (4) of the General Data Protection Regulation.

2. Thus, the Data Processor must not use another data processor (sub-processor) for the performance of the Data Processing Agreement without prior notice to the Data Controller.

3. Sub-processors are listed in Appendix B to this Agreement.

4. By entering into a sub-processor agreement, the Data Processor is responsible for imposing on any sub-processor at least the obligations that the Data Processor is itself subject to pursuant to the data protection regulations as well as this Data Processing Agreement with appendices.

5. If the sub-processor does not meet its data protection obligations, the Data Processor remains fully liable to the Data Controller for the performance of the sub-processor's obligations.

8 Transfer of Data to Third Countries or International Organisations

1. Unless required to do so by Union or Member State law to which the Data Processor is subject, the Data Processor must only process personal data subject to documented instructions from the Data Controller, including with regard to transfer (handover, disclosure and internal use) of personal data to third persons. In this case, the Data Processor informs the Data Controller of this legal requirement before processing, unless that law prohibits such disclosure on important grounds of public interest, cf. Article 28(3)(a).

2. Thus, within the framework of the Data Processing Agreement, the Data Processor cannot, without the Data Controller's instructions or approval, among other things,

    a. disclose personal data to a data controller in a third country or an international organisation,
    b. entrust the processing of personal data to a sub-processor in a third country,
    c. have the data processed by another department of the Data Processor that is located in a third country.

9 Assistance to the Data Controller

1. Taking into consideration the nature of the processing, the Data Processor shall assist, to the extent possible, the Data Controller with appropriate technical and organisational measures for the discharge of the Data Controller's statutory obligation to respond to

requests for exercising the data subject's rights, as laid down in Chapter III of the General Data Protection Regulation.

This means that the Data Processor shall, to the extent possible, assist the Data Controller in making sure that the Data Controller ensures compliance with:

a. the duty of disclosure in connection with the collection of personal data from the data subject
b. the duty of disclosure if personal data are not 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. the obligation to provide information 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 result of automated individual decisions, including profiling

2. Taking into account the nature of the processing and the information available to the Data Processor, cf. Article 28(3)(f) of the Regulation, the Data Processor assists the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Article 32-36 of the General Data Protection Regulation.

   This means that the Data Processor shall, taking into account the nature of the processing, assist the Data Controller in making sure that the Data Controller ensures compliance with:

   a. the obligation to implement appropriate technical and organisational measures to ensure a level of security that successfully addresses the risk 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, within 72 hours of giving the Data Controller notice of the breach, unless it is unlikely for the breach of personal data security to involve a risk to the rights and freedoms of physical persons
   c. the obligation to — without undue delay — notify the data subject(s) of any breach of personal data security when such a breach will likely pose a high risk to the rights and freedoms of physical persons
   d. the obligation to conduct an impact assessment for data protection if a type of processing will likely pose a high risk to the rights and freedoms of physical persons
   e. the obligation to consult the supervisory authority (the Danish Data Protection Agency) prior to processing if an impact assessment indicates that the processing

will pose a high risk in the absence of measures taken by the Data Controller to mitigate the risk

3. Payments in connection with the assistance provided by the Data Processor to the Data Controller will be made at the Data Controller's expense and according to the sales and delivery terms and hourly rates of the Data Processor that are applicable at any time.

10 Notification of Breach of Personal Data Security

1. The Data Processor shall notify, without undue delay, the Data Controller of any and all cases where the Data Processor has been made aware of a breach of data protection security on site at the Data Processor's or any sub-processor.

   Notice by the Data Processor shall, if possible, be given to the Data Controller, within no more than 48 hours of the Data Controller's notification of the breach in order to give the Data Controller the option to comply with any possible obligation to notify the supervisory authority within 72 hours.

2. In accordance with section 10.2.b of this Agreement, the Data Processor — taking into account the nature of the processing and the information available to it — shall assist the Data Controller in reporting the breach to the supervisory authority.
   This can mean that the Data Processor shall, among other things, help provide the following information, which, pursuant to Article 33(3) of the General Data Protection Regulation, shall be included in the Data Controller's notice to the supervisory authority:

   a. The nature of the breach of personal data security, 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 breach of personal data security
   c. Measures taken or proposed to deal with the breach of personal data security, including, where relevant, measures to mitigate its potential adverse effects

11 Erasure and Return of Data

1. Unless Union or Member State law requires storage of personal data, upon termination of the services relating to processing, the Data Processor is obliged to erase or return all personal data to the Data Controller, at the Data Controller's own choice, and to erase any existing copies.

12 Supervision and Audit

1. The Data Processor shall make available all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the General Data Protection Regulation and this Agreement to the Data Controller and shall allow for and contribute to audits,

including inspections conducted by the Data Controller or another auditor mandated by the Data Controller. Any assistance provided by the Data Processor in this context shall be rewarded by the Data Controller according to the applicable hourly rates and business terms of the Data Processor and on current account.

2. The Data Processor is obliged to give authorities that have access to the Data Controller and Data Processor's facilities in accordance with the legislation applicable at any time, or representatives acting on such authorities' behalf, access to the Data Processor's physical facilities on proof of identity.

13 Duration and Termination

1. This Data Processing Agreement shall apply for as long as the Data Processor processes personal data on the Data Controller's behalf in pursuance of the Agreement. The Data Processing Agreement expires automatically on termination of the Agreement.

2. Upon expiration of this Agreement, the Data Processor erases, returns or stores the personal data processed on the Data Controller's behalf, as agreed with the Data Controller.

3. To the extent required by law that is subject to the same technical and organisational security measures that are stipulated in this Data Processing Agreement, the Data Processor can withhold personal data after this Agreement's termination.

4. Any assistance provided by the Data Processor in this context shall be rewarded by the Data Controller according to the applicable hourly rates and business terms of the Data Processor and on current account.

Appendix A Information on Processing

A.1 The purpose of the Data Processor's processing of personal data on the Data Controller's behalf is:

The Data Processor makes systems available to the Data Controller. The systems support the use of automated self-service devices and other self-service payment solutions by end-users.

A.2 The processing of personal data by the Data Processor on the Data Controller's behalf primarily relates to (nature of the processing):

The systems that the Data Processor makes available to the Data Controller are designed for the administration of purchase data. The functionality of these solutions comprises database solutions for storage of data, client programs for monitoring of data, physical terminals for interaction with end-users as well as communication solutions between terminals and server solutions.

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

Personal data processed by the Data Controller is data about purchases and shopping habits. These are usually pseudonymised data, where data can only be attributed to the data subject using other data from an external system that is not stored by the Data Processor. In some cases, data will include number plates and data that enables payments in connection with the use of charge/membership cards (e.g. name, address).

The systems the Data Processor makes available to the Data Controller do not contain any personal data about race, ethnicity, political, philosophical or religious beliefs, information that a person is suspected, accused or convicted of a crime, health information, sexual orientation, membership in trade unions or genetic or biometric data. The information further does not contain data about personal ID numbers.

The recorded data belongs to the category of data about the Data Controller's end-users.

A.4 The processing covers the following categories of data subjects:

The data subjects are persons who have a client relationship with the Data Controller.

A.5 The processing of personal data on the Data Controller's behalf can commence after the coming into force of this Agreement. The processing has the following duration:

The processing is not limited in time, and the data subject's data is saved for as long as it is relevant for the purchase relationship between the data subject and the Data Controller.

Appendix B Terms and Conditions for the Use of Sub-Processors by the Data Processor

B.1 Terms and conditions for the use of possible sub-processors by the Data Processor

To guarantee as much stability and security for the data as possible, the Data Processor uses sub-processors, and the Data Processor's systems are hosted in an external data centre. The Data Processor has the Data Controller's general authorisation to use sub-processors such as DIBS, Nets and an external data centre for hosting of data.

B.2 Sub-processors used

At the time of coming into force of the Data Processing Agreement, the Data Controller is informed of the use of the following sub-processors:

Name	Place/Country	Region	Assists with
VIVA-IT	Denmark	EU	Infrastructure
Nianet	Denmark	EU	Data storage, ERP
Global Connect	Denmark	EU	Data storage, servers
DIBS	Denmark	EU	Data storage and transaction processing
Nets	Denmark	EU	Data storage and transaction processing
NPS A/S	Denmark	EU	Transaction processing

Appendix C Instructions Concerning the Processing of Personal Data

C.1 Subject-matter of / instructions for the processing

The Data Processor processes personal data on the Data Controller's behalf by making systems available to the Data Controller. The systems support the use of automated self-service devices and other self-service payment solutions by the end-users.

C.2 Processing security

The Data Processor has partnered with sub-processors to ensure secure and robust data processing. The data will be physically placed in external data centres or in the Data Processor's own server rooms. The Data Processor continuously receives statements from sub-processors that ensure that the sub-processors meet the Data Processor's policies in the mentioned areas. The Data Processor's policies with regard to data security relate to:

Physical security of data

Access control

Personal access card and/or code is required to access the facilities where the data is located.

Power, cooling and fire protection

The resources necessary for maintaining the operations will be provided by subcontractors or in the data processor's own server rooms, including UPS systems, temperature monitoring and cooling systems.

System security

Monitoring

The Data Processor's subcontractor and the Data Processor itself have implemented internal procedures that ensure that alerts and alarms are handled with an eye to reacting to relevant events and acting accordingly.

Firewall — DDoS attacks

The access to data is ensured with a firewall that controls which IP addresses communicate at which ports, as well as with address conversion. Additional server functionality that prevents DDoS attacks by continuously monitoring and comparing incoming traffic between systems.

Backup & Restore

The Data Processor's subcontractors, in the form of external data centres, and the Data Processor continuously ensure that backup and restore are possible.

Data security

Logging of transactions

User transactions, exceptions and security events are logged, and logs are stored indefinitely.

Encryption and pseudonymisation

Traffic between servers and diverse devices in the data processor's systems is realised via encrypted data connections.

Access to data in the system

Access to the server is realised via VPN connections. The Data Processor's developers require a personal username and passwords to be able to access the production server.

Intervention

Access to rectifying and erasing data at the data subject's request is provided via administration programs.

Staff Safety and Security

The Data Processor has made sure that all employees and sub-contractors have grasped their responsibilities and are competent to perform their roles.