

1. Subject matter of these GTCs

- 1.1 By setting up and providing a connection for electronic systems to an Internet platform for transaction handling, Nexi Germany GmbH (hereinafter referred to as "Nexi") provides the Contractual Partner with a service that receives transaction-relevant data from the Contractual Partner's business and forwards such data to banks or payment service providers or third-party providers chosen by the Contractual Partner and/or processes the same. The prerequisite for forwarding is a corresponding order by the Contractual Partner as well as technical availability.
- 1.2 Nexi acts exclusively as a technical service provider between the Contractual Partner, the Contractual Partner's customers and the banks and/or payment service providers regarding the handling of the payment transaction. The payments themselves are executed directly from the banks or payment service providers to the Contractual Partner without Nexi having any influence on the payment or the information transmitted in the process, and without forwarding or receiving payments itself. The modalities of these payments shall be governed by separate contracts entered into between the Contractual Partner and the banks and payment service providers.

2. Scope

- 2.1 By entering into the Service Agreement, the Contractual Partner agrees to and accepts that these General Terms and Conditions shall govern its contractual relationship with Nexi to the exclusion of any and all other terms and conditions. Apart from these General Terms and Conditions, the basis for the contractual agreement for the respective service of Nexi is the respective Service Agreement.
- 2.2 The service-specific or product-specific additional conditions, provided they have expressly become part of the Agreement, shall take precedence over in the case of any contradictions. Deviating mandatory statutory provisions shall take precedence, deviating provisions between Nexi and the Contractual Partner shall take precedence only if agreed in writing in an individual agreement.
- 2.3 Any representation of particular qualities ("Guaranteed Condition"), i.e. as an exception of the limitation of liability referred to under Section 9, shall require express and written confirmation (i.e. the identification of the subject matter of the Agreement and the contractually agreed provisions regarding the qualities alone shall not suffice). The general description of deliveries and services by NEXI in catalogues, brochures and the product description on the website shall not be deemed a representation of qualities within the meaning of the law.

3. Requirements to be fulfilled by Contractual Partner

- 3.1 For individual services the Contractual Partner requires conditions that are to be established by him through contracts with third-party providers.
- 3.2 In particular, the modalities for handling the payment transactions shall be governed by third-party contracts entered into directly between the Contractual Partner and the banks or payment service providers. The payment transactions governed by third-party contracts shall take place directly between the banks or payment service providers and the Contractual Partner without Nexi having any influence on the contractual relationship, the payment or the information transmitted in the process, such as in the case of acceptance contracts for credit card payments. The contractual relationship with Nexi does not establish such acceptance right but presupposes one.
- 3.3 Nexi therefore cannot be held liable for the contents of such contractual relationships or for errors in the execution of payment transactions under such contractual relationships.
- 3.4 The Contractual Partner shall on its own responsibility provide for the technical connection of its system and its requirements to the Nexi Merchant Interface. Nexi can recommend service providers for this, but accepts no liability whatsoever for the contents or existence of contracts, even if these are brought about by way of Nexi's referral.

4. Nexi's services

- 4.1. General service obligations
 - 4.1.1 The service shall cover the set-up and parameterisation of the merchant configuration (Nexi Merchant Interface) on Nexi's Internet platform for the purpose of transaction handling for the products selected in the Service Agreement and at the price agreed in such Service Agreement.
 - 4.1.2 Nexi shall grant the Contractual Partner a limited-term right to use the Nexi Merchant Interface for the duration of the Agreement for the selected product at the respective price agreed in the Service Agreement (see Section 5).
 - 4.1.3 Moreover, the service shall cover the technical handling of individual transactions in the context of the selected product at the agreed transaction price.

4.1.4 The specific scope of the service shall encompass the products selected in the Service Agreement as well as further additional conditions that may apply to the respective products.

4.1.5 General technical changes, amended conditions or other requirements on the side of Nexi (and which constitute justified grounds for change), the Contractual Partner, the customer or third parties (credit card companies, credit institutions, banks, etc.) affecting the interface or the upstream system can necessitate measures for changes, adaptations or reprogramming with the Contractual Partner. Nexi is not obligated to render such services.

4.1.6 If no separate service level agreement (SLA) was agreed for consultation, Nexi is not obligated to adhere to particular service parameters (e.g. response or call-back times).

4.1.7 Nexi is entitled to use third parties or subcontractors to render the service.

4.2 Service level

4.2.1 Nexi shall render its service to the Contractual Partner and shall use all reasonable efforts to maintain a high availability of the technical service. The Contractual Partner acknowledges, however, that the accessibility and the functionality of the technical service depend decisively on the functionality of third-party systems, in particular the technical systems of the banks and other service providers as well as the availability of the Internet. Nexi cannot guarantee the full availability of the technical service at all times in the case of a malfunction, failure or other problems in such third-party systems.

5. Right of use and other intellectual property rights

5.1 Depending on the service package selected and within the limits of the provisions of the Service Agreement, Nexi grants the Contractual Partner a non-exclusive right to use the Merchant Interface provided by Nexi to the extent that is absolutely necessary for setting up and managing its Contractual Partner connection and its access to the Nexi backend system. Nexi reserves the right to adapt the Merchant Interface at any time, to provide a new version to the Contractual Partner or to change and also restrict the functions and properties of the Merchant Interface.

5.2 The right of use specified in Section 5.1 is tied to the Contractual Partner and shall not be transferred or passed on in any other way by the Contractual Partner without the prior written consent of Nexi, nor shall be otherwise transferable. The right of use shall not include ownership rights of any kind, nor shall it grant any rights in the source code or any decompiled software. The interface may be used only by the Contractual Partner himself, not by third parties.

6. Obligations of the Contractual Partner, security and checking

6.1 The Contractual Partner is aware of the elementary importance of adherence to the security regulations. Detailed information about security regulations to be adhered to can be found in the PCI DSS rules (Payment Card Industry Data Security Standard: www.pcisecuritystandards.org), which are also available on the websites of Visa or MasterCard and which are expressly acknowledged and adhered to by the Contractual Partner. The provisions of Nexi Germany GmbH's Terms and Conditions for Acceptance and Settlement of Credit and Debit Cards shall continue to apply in each case with regard to the current PCI requirements. The Contractual Partner shall in particular ascertain that all systems which communicate with the Nexi Merchant Interface or receive, forward or further process data via it are fundamentally suitable for this purpose and at all times meet the latest standards of technology (including with update and patch level) and effectively protected against unauthorised access by appropriate technical and organisational measures (e.g. physical access, system access and application access control measures, also with firewall and anti-virus protection). The Contractual Partner shall make available all necessary information for the technical handling of payments via the Nexi Merchant Interface or provide this information on request.

6.2 The Nexi Merchant Interface offers the Contractual Partner various possibilities to check its configuration and transaction data via an access to the Nexi backend system by which the Contractual Partner can check the conformity of its transactions (e.g. payments) handled via the Nexi Merchant Interface to its own system data. The Contractual Partner shall set up suitable processes for checking its transaction data and to use them regularly, at least once per month. He shall be liable for all damages and losses arising from failure to fulfil its checking obligations. The Contractual Partner acknowledges that insufficient checking of the transaction data can also result in third parties (e.g. banks and payment service providers) suffering damages or losses.

Terms and Conditions for Nexi Paygate

- 6.3 In addition, the Contractual Partner shall transmit to NEXI, in a correct and processable condition, all data necessary for the performance of the Agreement and inform Nexi without undue delay in writing about any changes to its master data as well as all disruptions, defects or other impairments with a sufficiently detailed description, including the consequences.
- 6.4 The Contractual Partner shall handle all complaints of its customers falling within its own contractual relationship directly with the customers. The Contractual Partner shall indemnify Nexi from claims of its customers.
- 6.5 The Contractual Partner shall make data backups himself within the legally permissible and/or prescribed scope. Unless expressly agreed in the Agreement, Nexi shall not be obligated to carry out data protection measures, data recovery measures or other support services. In particular, the Contractual Partner shall bear the costs as set out in the Service Agreement if Nexi has to render support services or other services that are obviously based on the fact that the Contractual Partner does not have any, or only insufficient, knowledge for using the systems and tools necessary for processing transactions.
- 6.6 The Contractual Partner warrants that he has full legal capacity and possesses the necessary permits to sell its products/services using the services of Nexi.
- 6.7 The Contractual Partner warrants that he shall use the services of Nexi exclusively for its own commercial purposes and for transactions for its own benefit. The Contractual Partner is the sole party to the contracts for the connection to the related third-party systems (e.g. service providers, acquirers, banks and payment service providers). He warrants that he is not acting as a middle man. The Contractual Partner shall handle complaints directly with its customers himself.
- 6.8 Before using Nexi's services, the Contractual Partner shall request information with regard to the adequate handling of transactions from the banks, payment service providers and/or third-party providers that he has selected and with whom he must enter into separate contracts. Furthermore, the Contractual Partner undertakes to adhere to the conditions and provisions of use of such service providers. In addition, the Contractual Partner shall transmit to Nexi, correctly and in a processable condition, all information from these service providers that is required for the smooth handling of transactions or is otherwise relevant for Nexi's services. Such third parties and the Contractual Partner shall be solely responsible for the smooth handling of the cash flow in payment transactions.

7. Payment modalities

- 7.1 The level of usage and service fees are set out in the Service Agreement as well as the Schedule of Prices and Services of Nexi in its currently valid version. All prices are exclusive of statutory VAT at the time of the service provision. The rent and transaction charges shall be due for payment at the end of the month. All accrued charges shall be due for payment in each case at the latest on receipt of the invoice, unless a particular date is specified. For the duration of the contractual relationship, the Contractual Partner shall maintain a SEPA direct debit mandate in favour of Nexi. Without such mandate, Nexi shall have the right to charge the Contractual Partner separate fees pursuant to the Schedule of Prices and Services or based on the costs incurred for expenses. Nexi shall further have the right to terminate the contractual relationship for cause. Nexi shall be permitted set off any accruing fees, interest and other claims arising in favour of Nexi from the entire business relationship existing with the Contractual Partner with counterclaims of the Contractual Partner which the latter holds against Nexi. Invoicing shall take place according to the procedure selected by the Contractual Partner in the Service Agreement.
- 7.2 In the event of any default in payment attributable to the Contractual Partner, the Contractual Partner shall bear the entire damage caused by such default. In the event of a chargeback attributable to the Contractual Partner, the Contractual Partner shall also bear the costs associated with the chargeback. In the event that the Contractual Partner is in arrears with the payment of more than 2 monthly invoices, Nexi shall also have the right to suspend the services unless the Contractual Partner settles the payment arrears within a further period of one month from such suspension being threatened and punctually meets its obligations.
- 7.3 Nexi shall have the right to adjust the prices from time to time to reflect changes in economic, technical or legal conditions giving rise to significant additional costs. Nexi shall inform the Contractual Partner at least six weeks in advance in the case of an intended adjustment. If the Contractual Partner does not agree with the adjustment, he shall have the right to object to the increase in fees in writing within six weeks from being notified about the increase in fees.

Terms and Conditions for Nexi Paygate

For this purpose, the time when the objection is received by Nexi shall be decisive. After expiry of the time limit, an objection shall be excluded and the increase in fees shall become valid. In the event of an objection being made, Nexi shall have the right to terminate the Service Agreement for cause on six weeks notice.

- 7.4 Possible third-party costs (see also Section 3, e.g. routing costs, PIN authorisation, credit agencies, acquiring contracts) are not covered by this Agreement and shall be invoiced to the Contractual Partner by the respective third party.

8. Term, Termination of the Agreement

- 8.1 The contractual relationship shall commence on the first day of the month following the date of signing of the Service Agreement, unless expressly agreed otherwise in the Service Agreement. It shall run for an initial fixed term of at least 36 months and automatically renew on expiry of each fixed term for a further fixed term of at least 12 months unless terminated. The contractual relationship may be terminated in writing observing a notice period of three months to the end of a fixed contractual term. This shall not affect the right to termination for cause.
- 8.2 The Agreement may be terminated for convenience by Nexi in its entirety or with respect to individual services on three months' notice if a service is related to third parties or suppliers, or can no longer be offered by Nexi for technical or legal reasons or because the product is discontinued by the third party or supplier. In individual cases, Nexi shall also have the right to effect termination on a shorter notice period if the service provided by the third-party provider is verifiably no longer available.

9. Liability

- 9.1 Liability on the part of Nexi
- 9.1.1 Nexi's liability shall exist in the case of wilful intent and gross negligence. In the case of slight negligence, Nexi shall be liable only for breach of material obligations jeopardising the achievement of the purpose of the Agreement or the very fulfilment of which is a prerequisite for the performance of the Agreement and on which the Contractual Partner may rely (cardinal obligations). In all other cases Nexi's liability for slight negligence, without prejudice to liability for damages arising from injury to life, limb and health and for damages for which Nexi is liable by reason of a guarantee as to quality or condition (Beschaffenheitsgarantie) or under the German Product Liability Act (Produkthaftungsgesetz – ProdHaftG), shall be excluded.
- 9.1.2 Where obligations the very fulfilment of which is a

prerequisite for the proper performance of the agreement, and on the compliance with which the Contractual Partner normally relies and may rely, are breached by slight negligence, Nexi shall be liable up to an amount equal to the fees paid by the Contractual Partner to Nexi in the previous six (6) months starting from the point in time of the damage event.

- 9.1.3 In derogation to this, Nexi shall be liable in the first three months from commencement of the Agreement for breach of a cardinal obligation by slight negligence up to an amount of 20,000.00 euros.
- 9.1.4 In derogation to the foregoing provisions, Nexi shall be liable in months four (4) to six (6) from commencement of the Agreement for breach of a cardinal obligation by slight negligence up to an amount equal to the fees which the Contractual Partner would be required to pay to Nexi for the first six (6) months from commencement of the Agreement as projected based on the fees to be paid in the first three (3) months from commencement of the Agreement.
- 9.1.5 In any case, Nexi's liability in the case of slight negligence shall be limited to the usual and typically foreseeable direct damage caused by Nexi in such cases.
- 9.1.6 Liability on the part of Nexi for loss of profit is excluded in the case of simple negligence.
- 9.1.7 Independent of the foregoing provisions, Nexi shall not be liable for
- a) damage due to inappropriate or improper use, or other use not provided for in the Agreement; incorrect operation; incorrect or careless handling or changes performed by the Contractual Partner or a third party without Nexi's prior consent;
 - b) exceedance of deadlines, unless these were acknowledged by Nexi as binding;
 - c) loss of interest incurred to the Contractual Partner due to late value dates;
 - d) network bottlenecks, outages and malfunctions that are caused by Deutsche Telekom or another network provider and their private branch exchanges;
 - e) outages or obstructions that are caused by authorisation schemes;
 - f) restoration of data, unless Nexi has caused its destruction intentionally or as a result of its gross negligence and the subscriber has ensured that these data can be reconstructed from other data sources (e.g. from keeping slips or documentation from back-ups) with reasonable effort.

Terms and Conditions for Nexi Paygate

9.2 Liability on the part of the Contractual Partner

The Contractual Partner shall be liable to Nexi for the following:

a) damage to property, financial loss and personal injury caused intentionally or negligently by it or persons it has authorised to fulfil its contractual obligations;

b) damage caused by improper or negligent/inappropriate handling, especially due to connecting third-party products without the consent of Nexi or the impact of third-party devices as well as the consequences of this; also with regard to complaints by cardholders and operators of authorisation schemes;

d) network bottlenecks, outages and malfunctions that are caused by Deutsche Telekom or another network provider and their private branch exchanges;

e) outages or obstructions that are caused by authorisation schemes;

f) restoration of data, unless Nexi has caused its destruction intentionally or as a result of its gross negligence and the subscriber has ensured that these data can be reconstructed from other data sources (e.g. from keeping slips or documentation or from back-ups) with reasonable effort.

10. Confidentiality/Advertising

10.1 The Contractual Partner shall maintain secrecy with respect to all data and information he has received or become aware of in the context of the Agreement, unless such data and information are expressly marked or intended for forwarding. The Contractual Partner further undertakes to make information accessible only to those employees or vicarious agents who directly require the information for the performance of the Agreement and who are bound by a corresponding confidentiality undertaking.

10.2 The Contractual Partner undertakes in particular to take measures to keep secret any passwords disclosed to him and to monitor such measures. Nexi shall be informed about such measures on request. The confidentiality undertaking shall not cover information (i) that was verifiably already known to the receiving party at the time of disclosure;

(ii) that is generally known, published, based on general expertise or state-of-the-art at the time of disclosure; (iii) that becomes generally known after the time of disclosure or becomes individually known to the recipient from third parties without breach of any confidentiality undertaking, statutory provision or official order; or (iv) that is independently identified or developed by the receiving party after the time of disclosure independent of the confidential information. The receiving party is not permitted to disclose confidential information of the disclosing party to third parties. Third parties in this context shall be any natural persons, legal entities, which are not affiliated with the receiving party under the legal provisions governing corporate groups pursuant to sections 15 et seq. of the German Stock Corporation Act (Aktiengesetz, AktG), as well as their employees and corporate bodies authorised to represent them. Disclosure to vicarious agents, subcontractors or external consultants of the receiving party shall be permissible only with the prior consent of the disclosing party.

10.3 The Contractual Partner grants Nexi a worldwide, non-transferable, non-exclusive right during the term of the Agreement to use the Contractual Partner's names, trademarks and company logo to promote the commercial relationship with the Contractual Partner for advertising and marketing purposes and to name the Contractual Partner as a reference customer on the Nexi website or in other media.

11. Data protection

11.1 The Contractual Partner is the data controller within the meaning of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) and is therefore responsible for ensuring compliance with all statutory data protection provisions arising from the GDPR and other statutory data protection provisions applicable to him.

11.2 Nexi acts as data processor in accordance with Article 28 GDPR on behalf of the Contractual Partner. For this reason, Annex 1 "Nexi Paygate Data Processing Agreement in accordance with Article 28 GDPR" to these GTCs contains a corresponding agreement on data processing that forms part of the present GTCs also with respect to Section 13.2. Conclusion of a separate agreement on data processing is not required.

11.3 As "Controller" pursuant to the GDPR, the Contractual Partner has an obligation, inter alia, to fulfil the statutory transparency duties towards data subjects and, to the extent required in the context of the services selected (e.g. in the context of creditworthiness checks with credit agencies), to obtain consents from data subjects.

Terms and Conditions for Nexi Paygate

12. Place of jurisdiction, applicable law

- 12.1 This Agreement and all legal relationships arising from the Agreement are governed by the laws of the Federal Republic of Germany to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG).
- 12.2 The courts with exclusive jurisdiction to adjudicate any disputes arising from or in connection with this Agreement shall be the competent courts of Frankfurt am Main.

13. Final provisions

- 13.1 Any changes or amendments to the contractual relationship between Nexi and the Contractual Partner shall require written form. This also applies to amendments relating to the written form requirement.
- 13.2 If individual provisions of the Agreement should prove invalid in whole or in part, this shall not affect the validity of the other provisions. The Parties shall replace the invalid clause by a valid clause that most closely approximates the purpose and economic intent the Parties pursued with the invalid clause.

Annex 1

Nexi Paygate Data Processing Agreement in accordance with Article 28 GDPR

Preamble

A contractual agreement relating to Nexi Paygate already exists between the Parties. The present Agreement clarifies the Parties' obligations under data protection law. It applies to all activities relating to Nexi Paygate in which employees of Nexi or third parties authorised by Nexi might come into contact with personal data of the Contractual Partner.

Nexi processes personal data on behalf of the Contractual Partner. Pursuant to the intent of the Parties and in particular that of the Contractual Partner, this Agreement contains the written authorisation for data processing within the meaning of Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR) and sets out the rights and obligations of the Parties in connection with data processing.

“Personal data” pursuant to Article 4(1) GDPR means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

Where in this Agreement the terms “data processing” or “processing” (of data) are used, their meaning shall be based on the definition of “processing” as referred to in Article 4 No. 2 GDPR. It refers to “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

1. Subject matter and term of authorisation

1.1 Subject matter

The subject matter of the authorisation is setting up and providing a connection for electronic systems to an Internet platform for transaction handling which receives transaction-relevant data from the Contractual Partner's business and transfers such data to banks or payment service providers and/or third-party providers chosen by the Contractual Partner and/or processes the same.

1.2 Duration

The duration of this authorisation (term) shall correspond to the term of the Service Agreement.

1.3

The Contractual Partner may terminate the Service Agreement at any time without observing a notice period in the event of a serious breach of the applicable data protection regulations or duties under this authorisation or if Nexi cannot or will not execute an instruction of the Contractual Partner.

2. Clarification of authorisation content

Nature and purpose of planned data processing

2.1

The Contractual Partner uses a payment platform for secure handling of payment transactions. This is an interface which enables the technical control of such payment transactions from various channels, e.g. in the case of payments over the Internet or online shops (e-commerce), payments using mobile devices such as smartphones or tablets, e.g. by means of in-app payment (m-commerce), or payments made via point-of-sale (POS) terminals, e.g. at check-outs, using mobile terminals or at ATMs). The personal data generated as a result are used for executing payments, preventing fraud, quality assurance as well as for support and analysis purposes.

For details on the scope, nature and purpose of the data processing, in particular the specifically authorised scope of services and payment types, reference is made to the respective principal agreement or agreements. Additional, albeit contractually non-binding details are furthermore set out in the respective product documentation.

The provision of the contractually agreed data processing shall take place exclusively in a Member State of the European Union or another signatory state to the Agreement on the European Economic Area. Any transfer to a third country shall require the prior consent of the Contractual Partner and shall be permitted only if the specific requirements of Article 44 ff. GDPR are fulfilled (e.g. adequacy decision of the Commission, standard data protection clauses, approved codes of conduct).

Terms and Conditions for Nexi Paygate

- 22 Categories of data subjects (persons or institutions which make payments to the principal and whose payment orders are processed in the system), account/card holders.
- 23 Types of personal data
Data for payment transactions falling under the following types of data:
- web server log data including IP addresses and time stamps,
 - amount,
 - currency,
 - payment method,
 - names of payment initiating persons/account-/card holders, if applicable
 - addresses of payment initiating persons/account/card holders (e-mail, invoice addresses, delivery addresses), if applicable
 - potentially used additional services (e.g. fraud prevention services),
 - information on the success or failure of a transaction,
 - other data types (Paygate parameters) which are required for the technical control of the respective payment method and potentially used additional services.

The data types (Paygate parameters) vary significantly in detail depending on the payment method or service used.

3. Technical-organisational measures

- 3.1 Within its sphere of responsibility, Nexi shall manage its internal organisation in such a way that Nexi meets the particular requirements of data protection. Nexi warrants that it has taken all required technical and organisational measures to ensure an appropriate level of protection of the Contractual Partner's data pursuant to Article 32 GDPR, in particular at least the measures specified in Annex 1.
- 3.2 The technical and organisational measures shall be governed by technical advances and further developments. In this regard Nexi shall be permitted to implement alternative adequate measures. At the same time, the defined measures must not fall short of the required level of security. Material changes shall be documented.
- 3.3 If the review/an audit of the Contractual Partner finds a need for adjustment, this shall be implemented by mutual consent.

4. Correction, restriction and erasure of data

- 4.1 Nexi may not correct, erase or restrict the processing of the data processed on behalf of the Contractual Partner of its own accord but only upon

documented instruction of the Contractual Partner. If a data subject turns directly to Nexi in this regard, Nexi shall forward such request to the Contractual Partner without undue delay.

- 4.2 To the extent covered by the scope of performance, the erasure concept, right to have data forgotten, erasure of data, data portability and provision of information shall be ensured by Nexi directly upon documented instruction of the Contractual Partner.

5. Quality assurance and other duties of Nexi

- 5.1 In addition to the compliance with the provisions of this contract, Nexi shall have statutory obligations pursuant to Articles 28 to 33 GDPR; in this regard, Nexi warrants in particular that it complies with the following requirements:

- Written appointment of a data protection officer who exercises its activity pursuant to Articles 38 and 39 GDPR. The contact details of the data protection officer shall be published on the contractor's website.
- Maintaining confidentiality pursuant to Article 28(3) second sentence lit. b), Article 29, Article 32(4) GDPR. For the performance of the work, Nexi shall use only those employees who have been bound by the confidentiality undertaking and have first been familiarised with the provisions on data protection of relevance to them. Nexi and every person subject to Nexi having access to personal data may process such data only in accordance with the Contractual Partner's instruction, including the authorisations granted in this Agreement, unless they are required to perform data processing by law.
- Implementation of and compliance with all technical and organisational measures required for this contract pursuant to Article 28(3) second sentence lit. c), Article 32 GDPR [details in Annex 1].

- 5.2 On request, Nexi and the Contractual Partner shall cooperate with the supervisory authority in the performance of their tasks.

- 5.3 Nexi shall inform the Contractual Partner of supervisory acts and measures of the supervisory authority without undue delay where such acts and measures relate to this contract. This shall also apply in cases where a competent authority investigates Nexi's data processing of personal data as part of an administrative or criminal procedure.

- 5.4 Where the Contractual Partner for its part is exposed to a supervisory procedure of the supervisory authority, to an administrative or criminal procedure, to the liability claim of a data subject or third party or to any other claim in connection with Nexi's data processing, the Contractual Partner shall make best effort endeavours to assist Nexi.

5.5 Section 7 of this Agreement sets out how the technical and organisational measures taken can be demonstrated to the Contractual Partner within the scope of the latter's monitoring powers.

6. Subcontracting

6.1 Subcontracts within the meaning of this provision shall mean those services which directly relate to the provision of the principal service. These shall not include ancillary services which Nexi uses e.g. as telecommunications services, postal/shipping services, maintenance and user service or the disposal of data carriers as well as other measures to ensure confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. To ensure data protection and data security of the Contractual Partner's data, however, Nexi shall implement adequate and legally compliant contractual agreements as well as monitoring measures also in the case of outsourced ancillary services.

6.2 The Contractual Partner hereby grants Nexi the general permission to avail itself of additional data processors for processing personal data of the Contractual Partner. In general, contracts with service providers relating to the auditing or maintenance of data processing procedures or equipment by other entities or other ancillary services, even if in this case access to the principal's data cannot be excluded, shall not be subject to permission as long as the contractor implements adequate provisions to protect the confidentiality of the principal's data.

6.3 Nexi shall inform the Contractual Partner in text form on four weeks' written notice before establishing additional sub-contractual relationships. The Contractual Partner may raise an objection to the change only for good cause which must be proven to Nexi. If the objection is not raised within 14 calendar days from receipt of the notification and not all good causes are expressly named by the Contractual Partner, the right to object to the establishment of the respective contract shall lapse. If an objection is justified, the Contractual Partner shall have the right to terminate the principal agreement on 3 months' notice.

6.4 The subcontractors, their registered offices and their services shall be published on the Nexi website for the respective service.

6.5 If the subcontractor provides the agreed service outside the EU/ the EEA, the Nexi shall take appropriate measures to ensure permissibility under data protection legislation. The same thing shall apply if service providers are to be used with the meaning of Section 6.1.

6.6 Within the scope of further outsourcing by the subcontractor, all contractual provisions in the contractual chain shall also be imposed on the further subcontractor.

7. Monitoring rights of the Contractual Partner

7.1 Prior to commencing data processing and thereafter at regular intervals, the Contractual Partner shall satisfy himself of the technical and organisational measures of Nexi. For this purpose he may e.g. obtain information from Nexi, arrange for submission of existing attestations by experts, certifications or internal audits or himself personally audit the technical and organisational measures of Nexi, if possible after timely consultation during normal business hours, or have such measures audited by a competent third party provided the latter is not a competitor of Nexi or of a company of the corporate group that includes Nexi. The Contractual Partner shall perform inspections only to the required extent and without disproportionately disrupting Nexi's business operations.

7.2 Nexi shall provide the Contractual Partner, upon the latter's written request within a reasonable period, with all information and documentation required to perform an inspection of the Contractual Partner's technical and organisational measures pursuant to Annex 1.

7.3 The Contractual Partner shall document the result of the inspections performed by him and notify Nexi thereof. The Contractual Partner shall inform Nexi immediately in the event of any errors or irregularities which the Contractual Partner identifies in particular in the review of contract findings. If during the inspection issues are found whose prevention in future require changes in the performance of the ordered procedure, the Contractual Partner shall notify Nexi of the necessary changes in the procedure without undue delay.

7.4 For enabling the Contractual Partner to perform inspections, Nexi may claim reasonable remuneration for the expenses incurred as a result.

8. Notification in the event of breaches by Nexi

8.1 Nexi shall assist the Contractual Partner with complying with the duties for the security of personal data, reporting duties in the event of data leaks, data protection impact assessments and prior consultations. These shall include but not be limited to:

Terms and Conditions for Nexi Paygate

- 8.1.1 ensuring a reasonable level of protection by technical and organisational measures which take account of the circumstances and purposes of the data processing as well as the anticipated likelihood and severity of a possible breach of law as a result of security gaps and immediately identifying relevant breaching events,
- 8.1.2 the obligation to report breaches of rules relating to the protection of personal data to the Contractual Partner without undue delay,
- 8.1.3 the obligation to assist the Contractual Partner within the scope of its duty to inform data subjects and to make available to him all relevant information in this regard without undue delay,
- 8.1.4 assisting the Contractual Partner in its data protection impact assessment,
- 8.1.5 assisting the Contractual Partner in the context of prior consultations with the supervisory authority.
- 8.2 For assistance services which are not contained in the scope of performance or not attributable to any misconduct on the part of Nexi, Nexi may claim a reasonable remuneration.

9. Contractual Partner's power to issue instructions

- 9.1 The Contractual Partner shall confirm oral instructions without undue delay (at least in text form).
- 9.2 The Contractual Partner shall inform Nexi without undue delay if he is of the opinion that an instruction is in breach of data protection regulations. Nexi shall have the right to suspend performance of the respective instruction until such time as it is confirmed or changed by the Contractual Partner.

10. Erasure and return of personal data

- 10.1 After the end of the principal agreement or at any time at the request by the Contractual Partner, Nexi shall return to the Contractual Partner all documents in hardcopy form, data, and data carriers it has provided to the latter or – at the request of the Contractual Partner, provided that no obligation to store personal data exists under Union law or the laws of the Federal Republic of Germany – shall erase the same. Nexi shall furnish documented proof of proper erasure.

- 10.2 The Contractual Partner shall have the right to have the complete and contractual return and/or erasure of data held with Nexi monitored in a suitable manner or have this verified by a knowledgeable third party provided such party is not a competitor of Nexi or of a company of the corporate group that includes Nexi.
- 10.3 Nexi undertakes to treat as confidential the information having become known to it in connection with the principal agreement, even beyond the end of the principal agreement.

11. Liability

- 11.1 For Nexi's liability under this Agreement, the liability exclusions and limitations pursuant to the principal agreement shall apply. Where third parties make claims against Nexi which originate from a culpable breach of the Contractual Partner against this Agreement or against one of its duties as controller under data protection law, the Contractual Partner shall indemnify Nexi from such claims on first demand.
- 11.2 The Contractual Partner shall indemnify Nexi from any and all fines imposed against Nexi on first demand in the Contractual Partner's has a share in the responsibility for the breach sanctioned by the fine.

12. Right of retention

The Parties agree that Nexi's right-of-retention defence within the meaning of section 273 of the German Civil Code (Bürgerliches Gesetzbuch – BGB) with respect to the processed data and the associated data carriers shall be excluded.

13. Final provisions

- 13.1 In the event that property of the Contractual Partner held with Nexi is jeopardised by measures of third parties (e.g. attachment or seizure), by insolvency proceedings or by other events, Nexi shall inform the Contractual Partner without undue delay. Nexi shall inform the creditors without undue delay of the fact that the data concerned are data which are being processed on behalf of another.
- 13.2 Written form shall be required for any side agreements.
- 13.3 Should individual parts of this Agreement be invalid, the validity of the remaining provisions of the Agreement shall not be affected thereby.

Terms and Conditions for Nexi Paygate

Annex 1: Technical-organisational measures

1. Pursuant to Article 32(1) lit. a) -d) GDPR, technical and organisational measures shall include, among others, the following:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. Pseudonymisation and encryption measures (Article 32(1) lit. a) GDPR; Article 25(1) GDPR)

2.1 Pseudonymisation

☒	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures
-------------------------------------	--

2.2 Encryption

☒	Encryption of data carriers in laptops / notebooks
☒	Shutting down computers for regular encryption of data carriers is forced by technical means

3. Confidentiality (Article 32(1) lit. b) GDPR)

3.1 Entry control

☒	Alarm system
☒	Securing of building shafts
☒	Automatic access control system
☒	Chip card/transponder locking system
☒	Locking system with code lock
☒	Manual locking system
☒	Video monitoring of accesses
☒	Light barriers/motion sensors
☒	Security locks
☒	Key rules

☒	Identity checks at reception
☒	Permanently locked doors
☒	Recording of visitors
☒	Careful selection of cleaning staff
☒	Careful selection of security staff
☒	Requirement to wear ID badges
☒	The data processing systems are located in a separate and secured room to which only selected employees of the IT department have access

3.2 Entry control

☒	Assignment of user rights
☒	Creation of user profiles
☒	Password assignment subject to complexity criteria and regular changes
☒	Authentication of username/password
☒	Assignment of user profiles for IT systems
☒	Use of VPN technology
☒	Blocking of external interfaces (e.g. USB)
☒	User of intrusion detection systems
☒	Encryption of mobile data carriers (e.g. USB sticks)
☒	Encryption of smartphone content
☒	Secure passwords for smartphones
☒	User of centralised smartphone administration software (MDM), for example for external erasure of data
☒	User of antivirus software
☒	Ongoing, automated process for security patches (WSUS)

☒	Encryption of data carriers in laptops / notebooks
☒	Use of a hardware firewall
☒	Use of a software firewall

3.3 Access control

☒	Existence of an authorisation concept
☒	Management of the rights by system administrator
☒	Number of administrators reduced to the necessary "bare minimum"
☒	Password policy incl. password length, password changes/password complexity
☒	Logging of accesses to applications, in particular for entering, changing and erasing data
☒	Encryption of data carriers
☒	Secure storage of data carriers
☒	Physical erasure of data carriers before re-use
☒	Proper destruction of data carriers (DIN 66399)
☒	Use of document shredders and/or certified service providers
☒	Documenting of shredding

3.4 Separation control

☒	Physically separate storage on separate systems or data carriers
☒	Logical client separation (software-based)
☒	Creation of an authorisation concept
☒	Encryption of data records which are processed for the same purpose
☒	Own file structures with corresponding authorisations
☒	For pseudonymised data: Separation of the map files and storage on a separate, secured IT system

☒	Definition of database rights
☒	Separation of production and test system

4. Integrity (Article 32(1) lit. b) GDPR)

4.1 Transfer control

☒	Setting up dedicated lines or VPN tunnels
☒	E-mail encryption (if requested by Contractual Partner)
☒	Encrypted file sharing system
☒	Use of an electronic signature
☒	Creation of an overview of regular access and transmission operations
☒	Documentation of recipients of data and the times of planned retention or agreed erasure deadlines
☒	In the case of physical transport: secure transport containers/packages
☒	Encryption of external data carriers if transferred (USB sticks, CDs, etc.)

4.2 Input control

☒	Logging of input, change and erasure of data
☒	Creation of an overview showing which applications can be used to enter, change and delete which data
☒	Traceability of input, change and erasure of data through individual usernames (not user groups)
☒	Storage of forms by which data have been taken over automated processing operations
☒	Assignment of rights for entry, change and erasure of data based on an authorisation concept
☒	Use of a document management system

5. Availability and resilience (Article 32(1) lit. b) GDPR)

☒	Uninterrupted power supply (UPS)
☒	Air conditioning system in server rooms

Terms and Conditions for Nexi Paygate

☒	Equipment for monitoring temperature and humidity in server rooms
☒	Protection power strips in server rooms
☒	Fire and smoke alarm systems
☒	Fire extinguishing system in server rooms
☒	Alarm signal for unauthorised entries to server rooms

6. Restoration ability (Article 32(1) lit. c) GDPR)

☒	Creation of a back-up & recovery concept
☒	Regular testing of data recovery
☒	Fast recoverability
☒	Creation of a contingency plan
☒	Storage of data back-ups at a secure, off-site location
☒	Server rooms not below sanitary facilities
☒	RAID systems, virtualisation

7. Process for regular testing, assessing and evaluating (Article 32(1) lit. d) GDPR; Article 25(1) GDPR)

☒	Data protection management;
☒	Incident response management (IT incident management, technical and organisational process in response to identified or suspected security incidents or disruptions).
☒	Data protection-friendly default settings (Article 25(2) GDPR);
☒	Contract monitoring No contract data processing within the meaning of Article 28 GDPR with corresponding instruction of the Contractual Partner, e.g.: clearly drafted contracts, formalised contract management, strict selection of service provider, duty to be satisfied in advance, follow-up checks.