PAYREXX AG
Burgstraße 18
CH-3600 Thun

Agreement on contract data processing

Order in accordance with Art. 28 GDPR

between	…… …… …… ……
hereinafter referred to as	Principal
and the company	**Payrexx AG** Burgstraße 18 CH-3600 Thun
hereinafter referred to as	Agent
Pertaining to	contract data processing over the Payrexx platform

1. Initial situation

Unless otherwise agreed, this agreement comes into force with the signing of both parties and is valid as long as the Agent processes personal data for the Principal.
The Agent processes personal data for the Principal pursuant to Art.4 no.2 and Art.28 GDPR on the basis of this order.

2. Scope, nature and purpose of the collection, processing or use of data

The scope, nature and purpose of any collection, processing or use of personal data, the nature of the data and the group of data subjects are described in Annex 1.

3. Technical and organizational measures according to Art. 32 GDPR (Art.28 Para.3 Clause 2 Letter c GDPR)

3.1. The Agent must implement the technical and organizational measures set out prior to the award of the contract and prior to the start of processing, in particular with regard to the specific execution of the order, and deliver them to the Principal for review (see Annex 2). If accepted by the Principal, the documented measures become the basis of the contract.

3.2. The Agent has security in accordance with Art. 28 Para. 3 Clause 2 Letter c, 32 GDPR, in particular in conjunction with Art. 5 Para. 1, Para. 2 GDPR. Overall, the actions to be taken are data security measures and the assurance of a level of protection appropriate to the level of risk with regard to the confidentiality, integrity, availability and capacity of the systems. In this context, the prior art, the implementation costs and the nature, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account.

3.3. The technical and organizational measures are subject to technical progress and further development. In that regard, the Agent is permitted to implement alternative adequate measures. In doing so, the safety level of the specified measures must not be undershot. Significant changes must be documented.

4. Correction, blocking and deletion of data

4.1. The Agent may not delete the data, which is processed in the order, on its own initiative or limit its processing. Insofar as a data subject directly addresses the Agent in this regard, the Agent will immediately forward this request to the Principal.

4.2. Insofar as included in the scope of services, the deletion concept, right to be forgotten, rectification, data portability and information according to documented instructions of the Principal are to be ensured by the Agent directly.

5. Quality assurance and other obligations of the Agent

In addition to compliance with the provisions of this order, the Agent is subject to statutory obligations in accordance with Art. 28 to 33 GDPR; In particular, it ensures compliance with the following requirements:

5.1. The Agent is Mr. Ivan Schmid, CEO is appointed as Data Protection Officer, privacy@payrexx.com. The Principal will be informed immediately of any change to the Data Protection Officer. The up-to-date contact details are easily accessible on the Agent's homepage.

5.2. The preservation of confidentiality pursuant to Art. 28 Para. 3 Clause 2 Letter b, 29, 32 Para. 4 GDPR. The Agent will use only employees who are committed to confidentiality and who have been previously familiarized with the data protection regulations that are relevant to them. The Agent and any person subordinated to the Agent who has access to personal data may process such data only in accordance with the instructions of the Principal, including the powers granted in this Contract, unless they are required by law to process.

5.3. The implementation and compliance with all technical and organizational measures required for this contract are in accordance with Art. 28 Para. 3 Clause 2 Letter c, 32 GDPR and Annex 2.

5.4. The Principal and the Agent work together with the supervisory authority to fulfill their tasks on request.

5.5. Immediate information to the Principal about control actions and measures of the supervisory authority, insofar as they relate to this order. This also applies insofar as a competent authority has determined in the context of an administrative or criminal procedure with regard to the processing of personal data during the contract data processing by the Agent.

5.6. Insofar as the Principal himself is subject to inspection by the supervisory authority, an administrative offense or criminal procedure, the liability claim of a data subject or a third party or any other claim in connection with the order data processing by the Agent, the contractor shall support him to the best of his ability.

5.7. The Agent will regularly review internal processes and technical and organizational measures to ensure that the processing within his area of responsibility complies with the requirements of applicable data protection law and ensures the protection of the data subject's rights.

5.8. Documentation of the technical and organizational measures taken against the Principal, which are to be taken from Annex 2 in accordance with Section 3.

6. Subcontracting conditions

For the purposes of this regulation, subcontracting CONDITIONS are those services that directly relate to the provision of the main service. This does not include ancillary services that the contractor uses, for example, as telecommunication services, postal/transport services, maintenance and user services as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Agent is obliged to take appropriate and legally compliant contractual agreements and control measures in order to ensure data protection and data security of the Principal's data, even with outsourced ancillary services. The subcontractors are described in Annex 1.

7. Control rights of the Principal

7.1. The Principal has the right to carry out inspections in consultation with the Agent or have them carried out by examiners to be named in individual cases. He has the right to convince himself of the compliance of this agreement by the Agent in his business through spot checks, which are usually to be registered in good time.

7.2. The Agent shall ensure that the Principal can convince himself of the compliance with the obligations of the Agent in accordance with Art. 28 GDPR. The Agent agrees to provide the Principal with the necessary information upon request and, in particular, to prove the implementation of the technical and organizational measures.

7.3. The proof of such measures, which do not only concern the specific order, can alternatively be made by the adherence to approved behavioral rules according to Art. 40 GDPR, the certification according to an approved certification procedure according to Art. 42 GDPR, current certificates, reports or statements drawn up by independent entities (such as accountants, auditors, data protection officers, IT security officers, privacy auditors, quality auditors) and/or appropriate IT security or privacy audit certification.

7.4. The Agent can assert a claim for remuneration in order to enable the checks to be carried out by the Principal.

8. Notification in case of violations of the Agent

8.1. The Agent shall assist the contracting authority in complying with the obligations on security of personal data, reporting of data breaches, data protection impact assessments and prior consultations, as set out in Articles 32 to 36 of the GDPR. These include, among others

8.1.1. the assurance of an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights by security vulnerabilities, and enable the immediate detection of relevant incidents of a breach

8.1.2. the obligation to report breaches of personal data immediately to the Principal

8.1.3. the obligation to support the Principal in providing information to the data subject and to provide him with all relevant information without delay in this connection

8.1.4. the Principal's support for their privacy impact assessment

8.1.5. the Principal's support in the context of prior consultations with the supervisory authority

8.2. For services that are not included in the terms of reference or are not the result of misconduct by the Agent, the Agent may claim a fee.

9. Authority of the Principal

9.1. Verbal instructions are confirmed by the Principal immediately (at least in text form).

9.2. The Agent must inform the Principal immediately if he believes a directive violates data protection regulations. The Agent is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the Principal.

10. Deletion and return of personal data

10.1. Copies or duplicates of the data are not created without the Principal's knowledge. This does not include backup copies, to the extent necessary to ensure proper data processing, and data required to comply with statutory retention requirements.

10.2. After conclusion of the contractually agreed work or sooner upon request by the Principal – at the latest upon termination of the service agreement – the Agent must deliver to the Principal all the documents that have come into his possession, the results of processing and utilization as well as data stocks which are in connection with the contractual relationship or, with the prior consent, destroy them in accordance with data protection. The same applies to test and scrap material. The Agent will inform the Principal upon request about the nature and the time of deletion.

10.3. Documentations serving as proof of orderly and proper data processing must be kept by the Agent according to the respective retention periods beyond the end of the contract. He can hand them over to the Principal for his discharge at the end of the contract.

11. Other agreements

11.1. Fees
A fee for this order is not required.
Insofar as the Principal requires support in accordance with section 4 for answering inquiries from interested parties, he shall reimburse the costs incurred as a result.
Insofar as the Principal is exercising control rights in accordance with Clause 7, the amount of the fee to be agreed in advance shall be based on a fixed hourly rate of the employee assigned to the Agent for support.

If the Principal issues instructions to the Agent in accordance with section 9, he shall be reimbursed for any costs arising from this instruction.

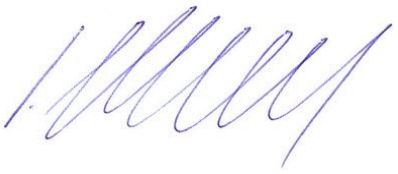
11.2. Contract duration
This agreement is dependent on the existence of a principal contractual relationship according to section 1. Termination or other termination of the principal contractual relationship pursuant to Number 1 also terminates this Agreement.
The right to isolated, extraordinary termination of this agreement and the exercise of legal rights of withdrawal specifically for the agreement remain unaffected.

11.3. Choice of law
It is the law of Switzerland.

11.4. Place of jurisdiction
The parties agree the registered office of the court responsible for Thun as the place of jurisdiction.

Signatures

……., the …….. Thun, 04/30/2018



…….. Ivan Schmid, Managing Director
Principal Agent

Annex 1 to the order according to Art. 28 GDPR

List of personal data and purpose of its processing

Type of data

The following data types and categories are subject of the additional agreement:

- Person master data
- Communication data (e.g. telephone, e-mail)
- Payment details (details on orders and payments made)
- Contract master data (contractual relationship, product or contractual interests)
- Information (e.g. credit check via payment provider)
- User behavior

Group of persons affected

The group of persons affected by this supplementary agreement includes:

- Customers and prospects of the Principal
- Employees and suppliers of the Principal

Involved subcontractors

These are service providers that relate directly to the provision of the main service.

Payrexx uses a number of external subcontractors to assist in the delivery of the main service.
Payrexx only uses trusted subcontractors.

Server environment

Amazon Web Services (AWS)
Server location: Germany (Frankfurt)
Privacy policy: https://aws.amazon.com/de/privacy

Customer management

Citrix Podio
Server location: Ireland (AWS)
Privacy policy: https://podio.com/site/privacy-policy

E-Mail Services

Mailgun
Server location: USA (AWS)
Privacy policy: https://www.mailgun.com/privacy-policy

MailChimp
Server location: USA

Privacy policy: https://mailchimp.com/legal/privacy

SMS Service

Twilio
Server location: Germany (Frankfurt, AWS)
Privacy policy: https://www.twilio.com/legal/privacy

Attached payment providers

PostFinance	Switzerland	https://www.postfinance.ch/privacyapp
PayPal	USA	https://www.paypal.com/ch/webapps/mpp/ua/privacy-full
PAYMILL	Germany	https://www.paymill.com/de/datenschutz
Stripe	USA	https://stripe.com/ch/privacy
Ingenico	Germany	https://ingenico.de/payment-services/service/datenschutz
Giropay	Germany	https://www.giropay.de/kaeufer/sicherheit-datenschutz
Concardis	Germany	https://www.concardis.com/ch-de/datenschutzerklaerung
Braintree	USA	https://www.braintreepayments.com/en-ch/legal
Sofort	Germany	https://www.klarna.com/sofort/datenschutz
BillPay	Germany	https://www.billpay.ch/de/datenschutz-ch
Twint	Switzerland	https://www.twint.ch/datenschutz-website
Saferpay - SIX	Switzerland	https://www.six-payment-services.com/de/shared/pages/six-privacy-statement.html
Datatrans	Switzerland	https://www.datatrans.ch/de/data-privacy
VIVEUM	Austria	https://www.viveum.com/datenschutzerklaerung
SWISSBILLING	Switzerland	https://www.swissbilling.ch/datenschutz
BS PAYONE	Germany	https://www.payone.com/datenschutz
WIRpay	Switzerland	https://www.wir.ch/rechtliche-hinweise
Mollie	Netherlands	https://www.mollie.com/de/privacy
Skrill	United Kingdom	https://www.skrill.com/de/fusszeile/datenschutz

		richtlinie
VR pay	Germany	https://www.vr-pay.de/datenschutz-haftung
WorldPay	United Kingdom	https://www.worldpay.com/uk/privacy-policy
CCAvenue	India	https://www.ccavenue.com/privacy.jsp
Razorpay	India	https://razorpay.com/privacy

Annex 2 to the order according to Art. 28 GDPR

Technical and organizational measures pursuant to Art. 30 Para. 1 Letter g in conjunction with Art. 32 Para. 1 GDPR

Confidentiality (Article 32 Para. 1 Letter b GDPR)

There is an access control (no unauthorized access to data processing systems).

This includes the following measures:

- Key / key assignment
- Door lock (electric door opener, etc.)
- Data center protected by Amazon Web Services: https://aws.amazon.com/de/compliance/data-center/controls/

There is an access control (no unauthorized use of the system).

This includes the following measures:

- Password procedure (including special characters, minimum length, regular password change)
- Two-factor authentication is used
- Automatic blocking (e.g. pause switching)
- Data center protected by Amazon Web Services: https://aws.amazon.com/de/compliance/data-center/controls/

There is a separation control / purpose control (separate processing of data collected for different purposes).

This includes the following measures:

- "Internal multi-client capability" is established
- Control of earmarking
- Separation of functions: Production, staging, testing

There is a pseudonymization of data records.

This includes the following measures:

- All personal data records are stored in an encrypted form.

Integrity (Art. 32 Para. 1 Letter (b) GDPR)

There is a relaying control (no unauthorized reading, copying, alteration or removal in case of electronic transmission or transport).

This includes the following measures:

- Secure SSL connection
- Assessment of the lawfulness of the information disclosure

There is an input control (determination of whether and by whom personal data has been entered, changed or removed in data processing systems).

This includes the following measures:

- Document management, document control
- Logging and log evaluation systems
- Plausibility checks
- Backup of log data against loss or change

Availability and capacity (Art. 32 Para. 1 Letter (b) GDPR)

There is an availability check (protection against accidental or willful destruction or loss).

This includes the following measures:

- Backup strategy
- Antivirus / Firewall

There is quick recoverability. This is guaranteed by the following measures:

- Emergency management including emergency plans
- 24/7 monitoring and telephone hotline
- Testing the recovery systems

Procedure for regular review, assessment and evaluation (Article 32 Para.1 Letter (d) of the GDPR, Article 25 Para. of the GDPR)

The technical and organizational measures were last evaluated on the following date:

04/25/2018

Process for the periodic review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing are in use.

This is supported by the following measures:

- Regular data protection training

The following instructions, regulations or analyzes are available in writing:

- Risk analysis
- Data protection concept
- List of processing operations
- Technical and organizational measures
- Subcontractor
- Contract data processing agreements
- Data protection statement