NEXARO

Agreement on Commissioned Data Processing

in the context of the provision of the Nexaro HUB

CONTRACTOR and PRINCIPAL for purposes of this agreement are the parties to the Contract on the Use of the Nexaro HUB and the services provided thereon for the management and control of devices (hereinafter referred to as "Nexaro HUB") on the basis of the general terms of use for the use of the Nexaro HUB (hub.nexaro.com) of Nexaro GmbH (hereinafter referred to as "Terms of Use"). The party referred to therein as the CUSTOMER is the PRINCIPAL, Nexaro GmbH is the CONTRACTOR of this agreement.

The execution of the contract involves the processing of personal data, which is why the parties supplement the contract by the content required pursuant to Article 28(3) GDPR. In order to comply with these requirements, the parties hereby enter into the following supplemental agreement on commissioned data processing:

§ 1 Scope of application and components of the agreement

(1) This agreement supplements the Contract on the Use of the Nexaro HUB, with the effect that the content becomes a constituent part of that contract. This agreement may survive the expiration of that contract to the extent provided for in the following provisions.

(2) The following annexes are a constituent part of this supplemental agreement:

Annex no.	DESCRIPTION
1	Categories of data subjects and data
2	Approved subcontractors
3	Technical and organizational measures

(3) In the event of any contradictions, the provisions in this agreement take precedence over the provisions of the Terms of Use.

§ 2 Details of the data processing

(1) The CONTRACTOR provides services for the PRINCIPAL in connection with the provision of the Nexaro HUB and the associated services and functionalities on the basis of the Terms of Use. Within the scope of the use of the Nexaro HUB, the CONTRACTOR will obtain access to personal data and shall process them on behalf of and in accordance with the PRINCIPAL's instructions. The duration of the processing corresponds to the duration of the provision of the contractual services.

(2) The nature and purpose of data processing by the CONTRACTOR are set out in the Terms of Use and the associated service descriptions.

§ 3 Right to issue instructions

(1) The CONTRACTOR may process data only within the scope of the contract for the use of the Nexaro HUB and in accordance with the instructions issued by the PRINCIPAL. If the CONTRACTOR is entitled to carry out any additional processing by virtue of the law of the European Union or of the member states to which the CONTRACTOR is subject, it has the right to do so (e.g., in order to comply with legal obligations to which the CONTRACTOR is subject). Prior to carrying out any processing based on statute but that is outside of the contract with the PRINCIPAL, the CONTRACTOR shall notify the PRINCIPAL on the legal requirements prior to the processing unless the CONTRACTOR is prohibited by law from providing such notification.

(2) The instructions of the PRINCIPAL shall initially be set out in this contract and may thereafter be amended, supplemented or replaced by the PRINCIPAL in writing or in text form by way of individual instructions. The PRINCIPAL is entitled to issue such individual instructions at any time. This includes instructions with regard to the performance of processing in individual cases, and in particular whether or not any processing shall be carried out. The right to issue instructions does not cover the selection of the means of processing and any technical or organizational measures of protection. The parties shall mutually agree such changes; the CONTRACTOR shall not unreasonably reject any changes requested by the PRINCIPAL.

(3) All instructions issued shall be documented by the PRINCIPAL. Instructions that go beyond the contractually agreed service shall be treated as change requests.

(4) If the CONTRACTOR is of the view that an instruction issued by the PRINCIPAL violates data protection provisions, the CONTRACTOR shall notify the PRINCIPAL without undue delay. The CONTRACTOR is entitled to suspend the execution of the instruction in question until it is confirmed or amended by the PRINCIPAL. The CONTRACTOR may refuse to carry out an instruction that is obviously unlawful. The confirmation or amendment of an instruction is only effective if it is issued in writing or in text form (e.g., letter, email, or fax).

§ 4 Type of data processed, group of data subjects

As part of the performance of the Contract on the Use of the Nexaro HUB, the CONTRACTOR is granted access to the personal data set out in *Annex 1*. The group of data subjects is also shown in *Annex 1*.

§ 5 Protective measures

(1) Within its area of responsibility, the CONTRACTOR shall structure its internal organization to ensure that it meets the specific data protection requirements. The CONTRACTOR shall take the necessary technical and organizational measures to appropriately protect the data of the PRINCIPAL, as set out in Article 32 GDPR, which ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services in connection with the processing. The PRINCIPAL is aware of the technical and organizational measures taken in accordance with

Annex 3 and responsible for ensuring that these measures provide a level of security appropriate to the risks to the data to be processed.

(2) The CONTRACTOR is entitled to change the security measures taken; the CONTRACTOR must ensure that the level of security does not fall below the level that was in place at the time the contract was entered into.

(3) The persons engaged in the data processing by the CONTRACTOR are prohibited from processing personal data without authorization. The CONTRACTOR shall place all persons entrusted with the processing and performance of this contract (hereinafter referred to as employees) under the same obligation (commitment to confidentiality, Article 28(3)(b) GDPR) and shall take reasonable steps to monitor compliance with this obligation.

(4) The CONTRACTOR has appointed a company data protection officer:

Nexaro GmbH
The Data Protection Officer
Mühlenweg 17–37, 42275 Wuppertal
Germany

The CONTRACTOR shall publish the contact details of the data protection officer on its website and notify the supervisory authority of these details. At the PRINCIPAL's request the CONTRACTOR shall provide suitable evidence of such publication and notification.

§ 6 Information obligations

(1) In the event of a personal data breach, the CONTRACTOR shall notify the PRINCIPAL without undue delay if data processed on behalf of the PRINCIPAL is affected.

(2) The CONTRACTOR shall take immediate measures to secure the data and to mitigate any possible adverse consequences for the data subjects.

(3) If data of the PRINCIPAL held by the CONTRACTOR is at risk of seizure or confiscation, or is threatened by insolvency or composition proceedings or other events or action taken by third parties, the CONTRACTOR shall notify the PRINCIPAL without undue delay unless the CONTRACTOR is prohibited from doing so by court order or official order. In this context, the CONTRACTOR shall notify all competent bodies without undue delay that the power to make decisions regarding the data lies solely with the PRINCIPAL in its capacity as "controller" as defined by the GDPR.

§ 7 Right of the PRINCIPAL to carry out checks

(1) The PRINCIPAL has the right to carry out checks at the CONTRACTOR—including on-site inspections. The subject of the right to carry out checks is compliance with the requirements of this contract and those laid down in Article 28 GDPR. The CONTRACTOR shall cooperate in the checks, e.g., by providing information, submitting any existing reports of experts, certifications, or

internal audits or by making the technical and organizational measures available for inspection after timely coordination during the usual business hours, which the PRINCIPAL may personally inspect or have inspected by a competent third party, provided that the third party is not in a competitive relationship with the CONTRACTOR. The PRINCIPAL shall carry out checks only to the extent necessary and shall not disproportionately disturb the CONTRACTOR's operations in the process.

(2) The CONTRACTOR undertakes to provide the PRINCIPAL, at the latter's verbal or written request and within a reasonable period of time, with all information and evidence required to carry out a check of the technical and organizational measures.

(3) The PRINCIPAL shall document the results of the check and inform the CONTRACTOR thereof. In the event that the PRINCIPAL discovers any errors or irregularities, in particular during checks of the order results, it shall inform the CONTRACTOR without undue delay.

§ 8 Use of subcontractors

(1) The CONTRACTOR is generally entitled to use third parties as additional processors for the provision of the services.

(2) Upon conclusion of the contract, the engagement of the subcontractors listed in *Annex 2* is expressly approved.

(3) The CONTRACTOR shall notify the PRINCIPAL of any intended change with regard to the engagement or replacement of another processor. The PRINCIPAL has the right to object to the new processor within 5 business days of receipt of such notification. If the parties fail to reach an agreement on the intended appointment of the new additional processor, the appointment will not be implemented.

(4) The CONTRACTOR is aware of and complies with the statutory obligations pursuant to Article 28(2) and (4) GDPR.

§ 9 Obligations to provide support

(1) Within the scope of the agreed services, the CONTRACTOR shall support the PRINCIPAL with any technical and organizational measures contained therein in the fulfillment of the PRINCIPAL's obligations to comply with the rights of data subjects.

(2) Furthermore, in due consideration of the type of processing and the information available to it, the CONTRACTOR shall support the PRINCIPAL in fulfilling its obligations under Articles 32 to 36 GDPR if and to the extent that the provision of such support is reasonable for the CONTRACTOR and indispensable for the fulfillment of the PRINCIPAL's obligations. Upon request, the PRINCIPAL and the CONTRACTOR shall cooperate with the supervisory authority in the performance of its duties.

(3) If a data subject asserts rights—such as the right to information, correction, or erasure with regard to their data—directly against the CONTRACTOR, the CONTRACTOR shall immediately refer the data subject to the PRINCIPAL.

§ 10 Liability

(1) In the internal relationship with the CONTRACTOR (*inter partes*), only the PRINCIPAL is liable to the data subject for compensation of any loss or damage suffered by a data subject due to any data processing or use during the commissioned data processing that is impermissible or incorrect pursuant to data protection law. This shall not apply if the CONTRACTOR has not complied with its obligations under data protection law as a processor in accordance with the GDPR or has acted in disregard of the lawful instructions issued by the PRINCIPAL or against the latter's instructions.

(2) The parties shall release each other from liability if one party shows that in accordance with paragraph 1, *inter partes*, it is not responsible. The same shall apply in the event of any contributory fault.

§ 11 Termination of the Contract on the Use of the Nexaro HUB

(1) Upon termination of the Contract on the Use of the Nexaro HUB or at any time upon the PRINCIPAL's request, the CONTRACTOR shall return all personal data to the PRINCIPAL and delete any remaining copies or—at the PRINCIPAL's request—delete the personal data. There is no obligation to delete personal data if the CONTRACTOR is obliged to store the personal data under European Union law or under the law of the Federal Republic of Germany.

(2) The CONTRACTOR is obliged to keep confidential any data of which it becomes aware in connection with the Contract on the Use of the Nexaro HUB, including after the Contract on the Use of the Nexaro HUB has terminated. This agreement shall remain valid beyond the end of the Contract on the Use of the Nexaro HUB for as long as the CONTRACTOR has not yet returned the personal data previously processed under the contract or deleted it at the request of the PRINCIPAL.

NEXARO

Annex no. 1

"Categories of data subjects and data"

Sequential no.	Data subjects	Data
1	**Users of the PRINCIPAL**	Company data: company name, postal address. User data: last name, first name; position and authorizations; role; telephone number; email address.
2	**Employees of the PRINCIPAL** (no users)	Company data: company name; postal address. Employee data: last name, first name; role; telephone number; email address. Object and device data: assigned objects and devices.
3	Third parties (customer contact of the PRINCIPAL)	Company data: company name; postal address. Contact details: last name, first name, role, telephone number, email address. Miscellaneous: assigned objects.

NEXARO

Annex no. 2

"Approved subcontractors"

Sequential no.	Company name and address	Role
1	**Vorwerk Elektrowerke GmbH Co. KG** Blombacher Bach 3, 42287 Wuppertal Germany	Intergroup (ESP tool, server hosting, 2FA service, 2nd-level support)
2	**Vorwerk Services GmbH** Mühlenweg 17–37, 42275 Wuppertal Germany	Intergroup (ERP system, e-commerce, ESP tool)
3	**intive GmbH** Prinz-Ludwig-Str. 17, 93055 Regensburg Germany	Development partner
4	**LetMeRepair GmbH** Fichtestraße 1 a, 02625 Bautzen Germany	Customer service and repair center (1st-level support)
5	**Vorwerk International & Co. KmG** Verenastrasse 39, P.O. Box 685, 8832 Wollerau Switzerland	Intergroup (Tools)
6	**ja-dialog Holding GmbH** Singerstraße 109, 10179 Berlin Germany	Customer service and repair center (1st-level support)

NEXARO

Annex no. 3

"Technical and organizational measures"

The processor shall implement the following technical and organizational measures for the protection of personal data. The individual categories are not exhaustive and can be supplemented if necessary.

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

1.1. Physical access control

The processor ensures that physical access controls are implemented at all locations where personal data is processed, whether at offices or data centers, in order to prevent unauthorized access.

1.2. Building security

All buildings are protected by access control systems.

In data centers or data processing rooms, additional controls such as humidity or fire detection systems, uninterruptible power supplies, and devices to protect against overvoltage or undervoltage shall be implemented.

All visitors must register at reception and be escorted when visiting one of the processor's sites.

1.3. Electronic access control

To prevent the unauthorized use of data processing and data storage systems, the processor has implemented various layers or protections depending on the device, authorizations, and location.

By default, all computers and mobile devices as well as data carriers and storage media are encrypted. Systems are automatically locked after a certain time and require secure passwords to be unlocked.

To access the processor's processing devices, all employees must have personalized accounts.

1.4. Internal access control (permissions for user rights to access and modify data).

The processor has implemented a role-based access concept.

1.5. Separation

Systems are designed to be multiclient capable.

2. Pseudonymization (Article 32(1)(a) GDPR; Article 25(1) GDPR)

Personal data is processed in such a way that the data cannot be linked to a specific data subject without the assistance of additional information, provided that such additional information is stored separately

and is subject to appropriate technical and organizational measures where required by the controller and compatible with the data processing activities.

- Isolation control: the isolated processing of data collected for different purposes

3. Integrity (Article 32(1)(b) GDPR)

3.1. Data transfer control

To protect data from unauthorized reading, copying, modification, or deletion, the processor has implemented controls to encrypt data in transit and supports the X.509 and PGP email encryption standards.

3.2. Data entry control

The processor has implemented systems or is part of information system solutions to verify whether and by whom personal data is entered, modified, or deleted in a data processing system.

The log files are structured to provide evidence of who added, changed, modified, or deleted data and when, and also to identify input errors and misuse.

4. Availability and resilience (Article 32(1) GDPR)

The processor has taken a variety of measures to ensure the availability and resilience of the data, in particular personal data, and to protect against accidental or intentional events such as destruction, power outages, lightning strikes, and fire and water damage.

4.1. Availability control

To protect against data loss, the processor has developed and implemented a backup policy to back up data on a regular basis. Backup media are stored at a physical location that is different from the location of the system.

In addition, the processor's information security systems are protected against attacks.

5. Procedures for regular testing, assessing, and evaluating (Article 32(1)(d) GDPR; Article 25(1) GDPR)

5.1. Data protection management

The processor has implemented processes and procedures to ensure that tasks are performed on time and that data can be backed up and restored.

5.2. Incident response management

In order to be prepared for all incidents, the processor has established an information security operations center to manage incident responses. In addition, the processor has developed, implemented, and tested

a cross-functional information security incident response plan to handle and manage information security incidents.

5.3. Order control

Data processing by third parties under Article 28 GDPR is not permitted without appropriate instructions from the processor, e.g., clear and unambiguous agreements, formalized contract management, strict controls in the selection of the service provider, pre-evaluation obligations, supervisory follow-up checks.

6. Organization

6.1. Appointment of a data protection officer

The processor has appointed an (internal/external) data protection officer to perform the advisory and supervisory roles. The contact details are accessible on the processor's company website at all times.

6.2. Further measures

The processor conducts regular training of its employees. All employees have been instructed on data protection and are obliged to ensure that personal data is handled in accordance with data protection law.