Data Processing Agreement in accordance with Art. 28 GDPR

between
Customer

---

the Controller – hereinafter referred to as the **Client** -

and
EMnify GmbH
Landsteinerstr. 4
97074 Würzburg

---

the Processor - hereinafter referred to as the **Supplier** -

Preamble

Within the meaning of Article 28 of the General Data Protection Regulation Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC, "GDPR", a contractual relationship exists between Client and Supplier.

Whereby Supplier provides telecommunications and other Services for the Internet of Things and in the area of Machine-to-Machine mobile radio communications only to business Customers and/or any potential business Customers (hereinafter jointly referred to as “Customer” or “Customers”) and not to private individuals, within the purpose of fulfilling its contractual duties and obligations, Supplier may process personal data within the meaning of the General Data Protection Regulation (GDPR) in the version applicable as of 25.05.2018.

The Supplier undertakes to the Client to comply with the Contract and this Agreement in accordance with the following provisions:

1. Subject matter and duration of the Contract

1) Subject matter

The Subject matter of the Contract results from the Terms of Service which is referred to here (hereinafter referred to as Terms of Service).

2) Duration

The duration of this Contract corresponds to the duration of the Terms of Service.

2. Specification of the Contract Details

1) Nature and Purpose of the intended Processing of Data

Nature and Purpose of Processing of personal data by the Supplier for the Client are precisely defined in the Terms of Service.

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled. The adequate level of protection in USA is the result of Standard Data Protection Clauses (Article 46 Paragraph 2 Points c and d GDPR).

California Consumer Privacy Act (CCPA)

If Supplier is processing Personal Data within the scope of the CCPA, Supplier makes the following additional commitments to Client. Supplier will process Client Data and Personal Data on behalf of Client and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale" exemption. In no event will Supplier sell any such data. These CCPA terms do not limit or reduce any data protection commitments Supplier makes to Client in the DPA Terms, Use Rights, or other agreement between Supplier and Client.

2) Type of Data

The Subject Matter of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories)

Personal Master Data (Key Personal Data): username and User ID (numeric ID), permission type, user creation date, MFA-Key (optional), hashed password, name, address, email address, phone number, IP-address when accessing the Supplier's portal, phone data (International Mobile Equipment Identity, IMEI lock, international mobile subscriber identity, integrated circuit card identifier).

Contact Data of Client's employees: Email-address, phone number, position, department, organizational assignment.

3) Categories of Data Subjects

The Categories of Data Subjects comprise: Customers.

3. Technical and Organizational Measures

1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organizational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in **Appendix 1**]

3) The Technical and Organizational Measures are subject to technical progress and further development. In this respect, it is permitted for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

a) Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. His/Her current contact details are always available and easily accessible on the website of the Supplier.

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organizational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in **Appendix 1**].

d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the

processing of personal data in connection with the processing of this Order or Contract.

f) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organizational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

6. Subcontracting

1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as postal / transport services, maintenance and user support services, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

2) The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client.

   a) The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company subcontractor	Address/country	Service / Task
AWS	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg	Deployment of the EMnify customer portal.
IDEMIA Germany GmbH	Konrad-Zuse-Ring 1 Flintbek 24220	SIM Cards

b) Outsourcing to subcontractors or changing the existing subcontractor are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

3) The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

5) Further outsourcing by the subcontractor requires the express consent of the Supplier (at the minimum in text form); All contractual provisions in the contract chain shall be communicated to and agreed with each additional subcontractor.

7. Supervisory powers of the Client

1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

    - Certification according to an approved certification procedure in accordance with Article 42 GDPR;

    - Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor)

    - A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO 27001 ISO/IEC 27001 (4) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

    a) Ensuring an appropriate level of protection through Technical and Organizational Measures that consider the circumstances and purposes of the processing as well

as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client

c) The duty to assist the Client about the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment

e) Supporting the Client with regard to prior consultation of the supervisory authority

2) The Supplier may claim compensation for support services which are not included in the description of the services, and which are not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

1) The Client shall immediately confirm oral instructions (at the minimum in text form).

2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

1) Copies or duplicates of the data shall never be created without the knowledge of the Client, except for back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection

compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

Appendix 1:
Technical and organizational measures, guaranteed by the processor

Appendix 1 - Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

1. Confidentiality (Art. 32 Par. 1 Point b GDPR)

a) **Physical Access Control;**
No unauthorized access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems;

Description of existent or taken measures by processor:
EMnify has physical access controls in place. These are: • Access control system (RFID) • Gatekeeper available • Video surveillance • Usage of visible ID-Cards • Regulations for visitors and guests • Safe areas and few access routes • Security staff and concierge • Smoke detector and sprinkler systems sufficiently available • Data center operations outsourced

b) Electronic Access Control;

No unauthorized use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media*;*

Description of existent or taken measures by processor:
The measures of electronic access controls are: • Use of unique IDs for all employees • Password policy defining password complexity requirements • Use of password manager • Enforcement of secure passwords • Multi-factor authentication in identity providers • Automatic blocking (e.g. wrong password, timeout) • Secure deposition of master and administrative passwords of all relevant IT systems • User rights are assigned to unique IDs • Usage of Mobile Device Management • Full-disk encryption of mobile devices and monitored via MDM • Usage of cryptographic methods that are state of the art, e.g., TLSv1.2+ • Data center operations outsourced • Regulation of data organization inclusive logging, reporting of data usage • Usage of data protection bin

c) Internal Access Control (permissions for user rights of access to and amendment of data); *No* unauthorized Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorization concept, need-based rights of access, logging of system access events*;*

Description of existent or taken measures by processor:
EMnify has internal access controls. These are: • Role-based access control in applications and cloud platforms • Inventory system for access permissions to applications • Periodical review of the access permissions • Differentiated access rights (e.g. profiles, roles, transactions and objects) • Concept / Documentation of access rights which could be audited • Workflow regarding assignment, change, modification and deletion of user access rights • Analysis of usage protocols and logs for API calls in cloud platform via AWS CloudTrail • Full-disk encryption of laptop hard disks and USB sticks

d) Isolation Control;

The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;

Description of existent or taken measures by processor:
The measures of isolation controls are: • Separation of development and productions systems • Network micro segmentation in production systems • Separated networks, e.g., unprivileged corporate network, production access based on zero-trust / end-to-end authentication

e) Pseudonymization (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR);

The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided

that this additional information is stored separately, and is subject to appropriate technical and organizational measures;

Description of existent or taken measures by processor:
Does not apply to the specific service due to the nature of the data processing.

2. Integrity (Art. 32 Par. 1 Point b GDPR)

a) **Data Transfer Control;**
No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature.

Description of existent or taken measures by processor:
The measures of data transfer controls are: • Full-disk encryption of laptop hard disks and USB sticks • Secure deletion or destruction of media • Encryption of data and data media in case of electronic transfer or transport (e.g. VPN, SSL/TLS) • Secure storage of SIM card key material through HSM-backed application-level encryption • Application-specific firewall rules through AWS Security Groups; • Periodic review of ports open to the Internet

b) **Data Entry Control;**
Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

Description of existent or taken measures by processor:
The measures of data entry controls are: • Logging and reporting systems

3. Availability and Resilience (Art. 32 Par. 1 Point b GDPR)

a) **Availability Control;**
Prevention of accidental or willful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning.

Description of existent or taken measures by processor:
The measures of availability control controls are: • Data center operations outsourced • Recovery Point Objective for critical data and other data • Recovery Time Objective for critical data and another data • Backups for corporate IT data as well as production databases; at least daily offsite backups • Usage of database clusters with built-in replication • Monitoring with automated alerting and 24/7 on-call personnel • Incident Response Policy • Disaster Recovery Plan • Regular Test Alerts • Virus scanners on Windows computers

b) **Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);**

Description of existent or taken measures by processor:
The measures of rapid recovery are: • Incident-Response Management with 24/7 on-call support • Disaster Recovery Plans • Fixed restart plan on a per-service basis • Defined responsibilities, processes and procedures

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

a) **Data Protection Management;**

Description of existent or taken measures by processor:
Demonstrable compliance with data protection regulation through • Company data protection is an ongoing compliance process • Appointment of an external Data Protection Officer • Appointment of an internal Information Security Officer • Ongoing update sessions regarding any changes or new data protection regulation • Setting up company data protection guidelines and • Continuous improvement process • Records of processing activities • Information requirements according to Art. 13 & 14 GDPR available • Contract management • IT Security policies • Internal regular Data Protection Awareness Training • Process for data breaches is available and documented • Data protection is included in the vendor management internal policy

b) Incident-Response-Management;

Description of existent or taken measures by processor:
Within its Incident Response Policy, EMnify has implemented a set of requirements for responding to a technical, availability, and/or security incidents whereby the roles and responsibilities for responding to any incident are clearly defined. Within this policy, the operational functioning of all critical system resources and supporting assets is assured. The four main categories of the Incident Response Policy include the following: • Initial Response and Containment • Analysis, Recovery and Repair • Communication • Post Incident Activities and Awareness • Internal information security officer

c) Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);

Description of existent or taken measures by processor:
• Automated data retention policies and processes on databases and storage system • System configuration can be restored through infrastructure as code • Usage of database clusters with built-in replication • Developers are trained in safe programming techniques

d) Order or Contract Control;

No third-party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalized Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

Description of existent or taken measures by processor:
The measures of order and contract control: • Unambiguous wording of the contract • Formal commissioning (request form) • Criteria for selecting the Processor / Service Provider • Monitoring of contract performance • Control checks and alignment with the Data Protection Officer

***