AGREEMENT ON PROCESSING ON BEHALF

regarding the agreement
Use of e-commerce platform SUPR
(„Main Agreement“)

between

SUPR Merchant (Shop Operator)
(„Controller“)

and

Wirecard Technologies GmbH
Einsteinring 35
85609 Aschheim
(„Processor“)

1. SUBJECT MATTER AND DURATION OF PROCESSING ON BEHALF

1) The present agreement for processing on behalf specifies the statutory rights and obligations resulting for the Controller and the Processor from applicable data protection legislation, in particular from the General Data Protection Regulation /Regulation (EU) 2016/679), in the following referred to as „GDPR“), as well as the applicable national implementing legislation, if and as far as the Processor processes personal data for the Controller within the scope of the Main Agreement.

2) The subject matter and purpose of processing on behalf of the Controller („Processing“) shall be the processing of electronic payment transactions as well as identity verification, fraud checks, anti-money-laundering prevention, risk management assessments and solvency assessments, to the extent the Controller has instructed the Processor with these tasks in the Main Agreement.

3) The duration of Processing shall comprise the term of the Main Agreement within the framework of which this Agreement on Processing on Behalf („Agreement“) has been concluded.

2. CONTENTS OF THE CONTRACT

1) The scope, nature and purpose of the intended collection, processing and use of data shall include
- fulfilment of the Processor‘s obligations resulting from the Main Agreement (use of SUPR platform);

2) The categories of data shall include
- Information about the end customer of the Controller (e.g. first and last name, address, e-mail address, date of birth, IP address)

The following data about the end customer of the Controller will be collected and processed:

- e-mail address
- Anrede
- surname / name
- invoice and delivery address
- IP address
- information of the chosen means of payment (e.g. credit card)
- information about the transaction (e.g. product, article number, costs of purchase and similar information which are stored and managed within the administratin area of the respective webshop)
- information about current and and past transactions of the end customer

to the extent this information is necessary for fulfilment of the above-referenced purposes.

3) The data subjects are be the Controller's end customers.

3. TECHNICAL AND ORGANISATIONAL MEASURES

1) To ensure that the Processing governed by the agreement specified above in the form concluded between the parties will be properly implemented by the Processor, the Processor has taken appropriate technical and organisational measures for data security within the meaning of Articles 28, 32 GDPR. The Appendix to this Agreement provides the Controller with an overview of the measures taken as of the date on which the contract is awarded.

2) The technical and organisational measures are subject to technical progress and further developments. In this respect, the Processor shall be permitted to further develop any measures taken and/or to replace them by adequate alternatives. In doing so, the degree of protection must not drop below the level of data protection prescribed by statute. Any significant changes shall be documented. The Processor will provide the Controller with information on the applied technical and organisational measures at any time upon request.

4. RECTIFICATION, BLOCKING AND DELETION OF DATA

The Processor shall support, within its possibilities, the Controller upon the Controller‘s instructions in its obligation to respond to requests for exercising the data subjects‘ rights pursuant to Chapter III GDPR and will implement the suitable and necessary technical and organisational measures. To the extent that any data subject directly addresses the Processor for the purpose of having his/her personal data rectified or erased, the Processor shall forward this request to the Controller. To the extent that the Processor supports the Controller in meeting the requirements of any data subjects, the Controller shall reimburse the Processor for the costs and expenses incurred.

5. OBLIGATIONS OF THE PROCESSOR

1) The Processor will process (including transfer) the personal data only upon instruction, i.e. the Controller‘s documented order instructing a specific handling of data by the Processor relevant under data protection laws (e.g. anonymization, blocking, deletion, submission), unless it is statutorily obliged to processing; in this case it will inform the Controller of this statutory requirement in advance, unless such information is prohibited based on an important public interest.

2) The Processor warrants that the employees used by the Processor for data processing purposes have been obliged in writing to observe data secrecy in accordance with Article 28 para 3b) GDPR or are subject to appropriate statutory confidentiality. To the extent that the Controller is subject to any further confidentiality obligations, for example in accordance with any regulations under professional law, criminal law or procedural law, the Controller shall inform the Processor thereof and shall, upon request, educate the Processor and the latter's employees on the application of the confidentiality obligations.

3) The technical and organisational measures, as defined in clause 3 of this Agreement and the corresponding appendix, are implemented and complied with by the Processor. This includes in particular

- Pseudonymisation and encryption of personal data
- The ability to ensure, on a continuous basis, confidentiality, integrity, availability and reliability of the systems and services in relation to the processing of personal data;
- The ability to ensure availability of personal data and access to the data in case of a physical or technical accident;
- A procedure for regular inspection, assessment and evaluation of the efficacy of the technical and organisational measures for ensuring the security of processing.

4) To the extent that no conflicting procedural considerations exist, the Processor shall inform the Controller of any regulatory measures of the competent supervisory authority in accordance with Art 58 GDPR as well as on any court decisions in connection with Articles 83, 84 GDPR.

5) The Processor appointed a data protection officer and will name him/her to the Controller in writing or via email.

6) The Processor shall be obliged to provide the Controller with information at any time to the extent that this affects the personal data and documents transferred by the Processor. Any data that is no longer required shall be erased at Processor without undue delay in accordance with clause 4 of this Agreement. Any controls that extend beyond this Agreement shall be governed exclusively by the statutory regulations.

6. SUPPORT PURSUANT TO ART 32 – 36 GDPR

Upon request, the Processor shall support the Controller, within reason and taking into consideration the type of processing and the information available to it, in the Controller‘s compliance with its obligations pursuant to Art. 32 to 36 GDPR with appropriate technical and organisational measures. This concerns, inter alia, the data subjects‘ rights, security of processing, notification of breaches and respective information to the data subjects, support in case of inspections by a data protection authority, and in data protection impact assessments. The Controller will reimburse the Processor for all costs and expenses incurred in relation with this, unless the measures causing the costs/expenses were caused by the Processor. If the parties cannot agree on the extent of reimbursement, all costs and expenses that the Processor may have deemed necessary will be reimbursed in full.

7. ESTABLISHMENT OF SUB-PROCESSING RELATIONSHIPS

1) To render the contractual services, the Processor may award parts of the Processing to sub-contractors. The following sub-contractors has been instructed to render services relevant to the contract as of the date of conclusion of the contract:

Company sub-contractor	Address/country	Service
CleverReach® USA (Cam-paign Moni-tor)	154 Grand St New York, NY 10013 USA	Newsletter system / mail service of systemic generated emails
Slack	500 Howard Street, San Francisco, CA 94105, United States of America	Team-Chat (no end customer data stored only merchant data)
billwerk GmbH	Mainzer Landstraße 51 60329 Frankfurt am Main	Invoicing & claims management system
Freshworks Inc.	1250 Bayhill Drive Suite 315 San Bruno, CA 94066 USA	Helpdesk-SaaS / CRM-system
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109 United States	Hosting Wirecard infrastructure and mail service / Failo-ver-System. Only server in Europe/ Frankfurt

The Controller agrees to the sub-contracting to the aforementioned companies. The Controller also agrees to the sub-contracting to further companies provided the obligations of this Agreement are forwarded to the sub-processors and at least the same level of protection will be maintained.

2) In case of any involvement of any further sub-contractors, the Controller shall inform the Processor. In addition, the Controller may reject additional sub-contractors of the Processor only if there is any compelling reason under data protection law to do so and this has been communicated to the Processor in writing immediately after the information had been received. Sub-contractual relationships within the meaning of this provision shall not be deemed to include any such services of which use is made by the Processor from any third parties as an ancillary service for support in the implementation of the contract. This shall include, inter alia, telecommunication services including

housing, as well as any transfer and hosting of data, transport and communication services, cleaning staff, as well as any disposal of data carriers and documents.

3) Within the framework of the sub-contractual relationships, the Processor shall enter into any agreements required under data protection law. The Processor is permitted to process the data also outside of the EEA in compliance with the provisions of this Agreement, or to have them processed, provided that it informs the Controller in advance on the location of the data processing an evidences compliance with the technical and organisational measures. This section 7 shall fully apply to any sub-contractors. The Controller hereby authorises the Processor to enter into any agreements with sub-contractors, in representation of the Controller – including, but not limited to, (sub-)processing agreements and EU Standard Contractual Clauses or similar agreements – that are required to guarantee an appropriate level of data protection with regard to the transfer of data. The Processor may grant sub-contractors substitute powers of attorney. The Controller agrees to provide support in meeting the legal requirements of the transfer of data.

8. CONTROLLER'S RIGHTS TO MONITOR

1) The Controller shall convince itself that its personal data is properly processed and that the technical and organisational data security measures taken at the Processor's premises on site are complied with. To this end, the Processor shall, upon the Controller's request, demonstrate compliance with the technical and organisational measures by means of up-to-date certificates, reports or extract of reports of independent entities (such as internal audit, data protection officer, IT security department, external data protection auditors) or any certification by an IT security or data protection audit (e.g. in accordance with PCI DSS) and/or acknowledged certifications pursuant to ISO 27001.

2) The Processor shall enable and support the Controller or an external independent auditor instructed by the Controller, the review, including inspection, in particular if there was a security incident and/or a review, including inspection, is requested by the legislator or a data protection authority. The Controller or its instructed independent third party may access the premises of the Processor at which data pf the Controller are processed, after respective notice and during normal business hours, at its own cost and without interruption to the business operations, ensuring the secrecy of any trade or business secrets of the Processor and any potential sub-contractors, to convince itself of compliance with the technical and organisational measures of Appendix 1.

3) The Controller shall inform the Processor sufficiently in advance (usually at least four weeks) about all circumstances in relation to the carrying out of an inspection. The Controller may, as a rule, carry out one inspection per calendar year. This shall not affect the Controller‘s right to conduct further inspections in case of violations of data protection obligations of the Processor.

4) If the Controller instructs a third party with the inspection, the Controller shall oblige this third party in the same way as the Controller is obliged to the Processor under this Agreement. Upon request the Controller must provide the respective agreement with such third party to the Processor. The Controller must not instruct a competitor of the Processor with an inspection.

5) The Processor is permitted, in its own discretion and taking into account the statutory obligations of the Controller, to not disclose information that is sensitive with regard to the Processor‘s business or if the Processor would breach statutory or contractual obligations with the disclosure. In particular, the Controller will not receive access to information about other business partners of the Processor as well as about any other non-public information of the Processor that is not strictly required for the statutory inspection rights.

6) The Controller will reimburse the Processor for its costs and expenses in relation to the evidencing of compliance with the technical and organisational measures, in particular the expenses in relation to any reviews and inspections on its premises.

9. NOTIFICATION IN CASE OF INFRINGEMENTS BY THE PROCESSOR

The Processor shall promptly inform the Controller if it becomes aware of a breach of the protection of

personal data of the Controller. The Processor shall take the measures necessary to safeguard the data as well as to minimise any potential adverse consequences for any data subjects in coordination with the Controller.

10. CONTROLLER'S RESPONSIBILITY AND AUTHORITY TO ISSUE INSTRUCTIONS

1) The Controller shall be the controller for the processing of data on behalf by the Processor. The evaluation of the admissibility of the data processing shall be the obligation of the Controller. The Controller shall provide the Processor with the data in due time and in the required quality to ensure that the Processor will be able to render the services.

2) The Processor shall process the personal data provided to it within the framework of the instructions issued by the Controller as stipulated in the contract.

3) The Processor and its sub-contractors may process the data for their own purposes in accordance with data protection law, provided that this is permitted by statute or the data subject's consent. This Agreement shall not be applicable to any such data processing. In any case, the Processor and its sub-contractors may process the data for their own purposes in an anonymised form.

4) The Controller shall bear additional costs incurred due to any instructions; the Processor may request an advance payment. The Processor may refuse to carry out any additional or modified data processing if it would result in any change in the amount of work or if the Controller refuses to reimburse the additional costs or to make the advance payment.

5) For reasons of traceability, any instructions of the Controller shall be given in writing or in text form (e.g. by e-mail); any oral instruction shall be confirmed in writing or in text form without undue delay.

6) If the Processor considers that an instruction given by the Controller infringes the GDPR, the Federal Data Protection Act or any other data protection regulations, the Processor may refuse to execute the instructions until the Controller has confirmed the instruction or has changed it into an instruction that is in accordance with data protection regulations.

11. DELETION OF DATA AND RETURN OF STORAGE MEDIA

Upon the end of the contractual relationship, the Processor shall be obliged, at the Controller's option, to delete, to block or to return to the Controller any personal data that has been provided to the Processor in connection with the service agreement and has not yet been deleted by then. Any retention obligations, including but not limited to those in accordance with statutes, by-laws, contracts and regulatory instructions, shall remain unaffected.

12. POINT OF CONTACT FOR DATA PROCESSING AND DATA PROTECTION QUERIES

On the part of the Controller:

The SUPR merchant itself unless otherwise stated.

On the part of the Processor:

External data protection officer: Dr. Felix Wittern, Fieldfisher (Germany) LLP, Am Sandtorkai 68, 20457 Hamburg, Germany.

APPENDIX 1

TECHNICAL AND ORGANISATIONAL MEASURES (TOMs) OF WIRECARD GROUP

The Wirecard Group ("Wirecard") has taken appropriate measures to ensure an adequate level of security appropriate to the risk, having regard to the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons. To this end, Wirecard has taken into account the protection objectives of Art. 32 (1) GDPR, such as the confidentiality, integrity and availability of systems and services and their resilience with regard to the nature, scope, circumstances and purposes of the processing operations. Wirecard has also implemented a process for regular testing, assessing and evaluation the effectiveness of technical and organizational measures for ensuring the security of the processing.
The measures taken to ensure compliance with the individual controls are explained in more detail below.

Pseudonymisation (Art. 32 (1) a) GDPR)	As a rule, Wirecard uses encryption as a form of pseudonymisation where this is nec-essary and relevant.
Encryption (Art. 32 (1) a) GDPR)	As a general rule, the exchange and transmission of personal data only take place in encrypted form. When exchanging personal data, encryption is a key issue of the general data protection training courses which are mandatory for each member of staff. All interfaces to external bodies transferring personal data in automated form are secured in accordance with the latest standards, e.g. by TLS encryption. • Mobile computers (laptops) are equipped with hard disk encryption. • Depending on the way in which the data is transferred, encrypted transmission protocols via HTTPS, TLS v1.1 or v1.2 and SFTP, SSH v2,are used. • E-mails and files can be encrypted (e.g. PGP encryption for the regular, encrypt-ed exchange of data). • Credit card data is stored encrypted in Wirecard systems. • Wirecard uses strong encryption algorithms, which are stated in the internation-al security standards such as NIST and PCI DSS. • Encryption keys are protected from general access. Only approved custodians are able to access the encryption key components • Encryption keys generated using approved strong cryptographic algorithms for random or pseudo-random number generation and random prime number gen-eration, are stored in one of the following forms at all times: o Encrypted with a key-encrypting key (KEK) that is at least as strong as data en-crypting key; o As at least two full-length key components (no key custodian know or have ac-cess to all pieces of data-encrypting keys); o Within a secure cryptographic hardware device (HSM); • All data encryption keys are changed after they reach end of crypto period or when circumstances for example leaving of key custodians, dictate a change to maintain key integrity. • Development/test systems are separate from production environments with access control in place to enforce separation. • Production data (live PAN) are not used for testing purposes.

Confidentiality (Art. 32 (1) b) GDPR)	**Access to premises** • All premises of Wirecard have an access system in place based on chip cards. Distinction is made between entries to different areas within the buildings. All employees are provided with chip cards with access rights required for their work. Access rights granted centrally by the Facility Management department are documented, and reviewed by the IT Security department at regular intervals. Visitors must be accompanied when moving inside the office premises and are provided with separate identity cards. • All entries to Wirecard buildings are monitored by CCTV. • Access to data centres is subject to stringent regulations. Any access to the data centres requires a separate registration, which also applies to Wirecard employees. The registrations are made by heads of the IT department and in a manner protected against forgery (authenticated). • Third parties are allowed to enter the data centres only in exceptional cases and must be accompanied by Wirecard employees. Any access is logged in a revision-proof manner. The access logs are reviewed by the IT Security department at regular intervals. • The data centres are protected against unauthorised access, with security staff being on site 24/7 as well as by CCTV and alarm systems. **Control of access to systems** • All systems at Wirecard are equipped with access control systems. • Access to systems is personalised for each member of staff at Wirecard. Access is secured by personal passwords, only known to the respective employee. The Password Policy requires changing the personal password at regular intervals (depending on the system, periods of 90 days or less have been set) and ensures the quality and complexity of the password by means of specifically defined rules. All rules on the assignment and modification of passwords have been laid down in writing and are in compliance with the binding PCI-DSS regulations. • The screens of all workstations and all services processing or storing personal data are automatically blocked after 15 minutes of inactivity. De-blocking is only possible using the personal user password by repeated log-in. Moreover, any blocking of the workstation computer when leaving the workstation is regulated by an internal policy in a mandatory manner.

	Control of access to data • The access control is based on a system of roles and rights used to ensure the need-to-know principle of any access to data. Thus, each member of staff has ac-cess to precisely such data that he/she needs for his/her daily work. • The rights required for the employee's respective position have been defined in the form of roles assigned to the employee. Any further individual authorisa-tions have to be released by the IT Security department. Authorisation takes place after consultation with the information owner (as a general rule, the head of the responsible specialist department) and within the framework of the in-structions given under data protection law. • The assignment of rights is documented in a comprehensible manner. • The role descriptions and the rights assigned are documented and maintained by the responsible departments and are verified on a sample basis at regular in-tervals (at least once a year) by the IT Security department. • Administrator access authorisations are only granted after prior internal train-ing. Any administrator access to the systems is recorded in a revision-proof man-ner in accordance with PCI-DSS regulations. • The prevention of any unauthorised persons from gaining access to data is guar-anteed by installing security updates at regular intervals and in a prompt man-ner for all third-party applications used; the IT operating systems (OS) are pro-vided with monthly security updates in accordance with PCI-DSS regulations.

Integrity **(Art. 32 (1) b) GDPR)**	As a general rule, the exchange and transmission of personal data only take place in encrypted form. Depending on the way in which the data is transferred, encrypted transmission protocols via HTTPS, TLS v1.1 or v1.2 and SFTP, SSH v2,are used. E-mails and files can be encrypted (e.g. PGP encryption for the regular, encrypted ex-change of data). In addition, there is a system ensuring the secure one-time transmis-sion of personal data (data room principle). • When exchanging personal data, encryption is a key issue of the general data protection training courses which are mandatory for each member of staff. All in-terfaces to external bodies transferring personal data in automated form are se-cured in accordance with the latest standards, e.g. by TLS encryption. • All interfaces are documented. The external documentations of the interfaces are available. • Media inventories and a clean desk policy prevent the unauthorised inspection as well as theft of storage media and documents. As a general rule, storage me-dia and documents containing special personal data are sent by courier service, with the storage media being encrypted. • In the event of administrator access, all modifications made to personal data in the systems of Wirecard are recorded by the respective software application or documented on the basis of corresponding processes to ensure that all modifica-tions can be traced back at any time. • For the purposes of data input and modification, each member of staff has a personal user name for the respective system to ensure that all inputs can be at-tributed to a specific person. • The quality of any applications developed by Wirecard is ensured, prior to im-plementation, by a comprehensive quality assurance process.
Availability **(Art. 32 (1) b) GDPR)**	• Wirecard is operating two data centres at different locations which, in accord-ance with BSI requirements, are located at least 5 km away from each other to guarantee the highest level of fail-safe operation. Within each data centre, re-dundancy is built-in for all key system components. • The data centres are aligned to the TIER 3 standard of the Uptime Institute and are certified according to ISO 27001 or ISAE 3402; this guarantees appropriate measures to protect them against failures, and the processes tailored to this. • Backups of all data are created at regular intervals (daily) and are kept at a safe location separated by structural measures, with the requirements of the BSI (also regarding sabotage) being observed. • All systems are monitored around the clock to ensure that immediate action can be taken in any case of error. • As a service provider, Wirecard processes data for a large number of customers for payment processing in the context of data processing on behalf. Carefully granting access rights ensures that all data will only be processed in accordance with purpose limitation and the instructions given by the controller. • All relevant data is stored in the databases of Wirecard with a unique customer identification to ensure that unambiguous attribution is possible at any time. At the same time, test data is clearly separated from any productive data. • In addition, the stringent purpose limitation and separation of processing are ensured through regular training of the employees as well as by regular reviews carried out by the IT Security department.

Resilience of processing systems and services (Art. 32 (1) b) GDPR)	• A security assessment on the network configuration and firewall rule base occurs twice a year, and vulnerability scans/assessments every 90 days, as well as pene-tration tests at least once a year, are implemented on application and network layer as prescribed by PCI-DSS. • Wirecard is operating intrusion detection systems (IDS) and intrusion protection systems (IPS) and 24/7 stand-by duty ensures timely alerts in any case of failure (incidents). • All workstation computers are equipped with an anti-virus solution which is automatically and continuously updated. Mobile computers (laptops) are equipped with hard disk encryption.
Process to restore the availability and access to personal data in the event of a physical or technical incident (Art. 32 (1) c) GDPR)	• Back-up plans set up in line with the requirements of the systems hosted in Wirecard. Networker appliance is used to automate the back-up process. • Standard clients are backed up daily with a differential/incremental backup and weekly full backup is also performed. • The databases in the primary data center are duplicated into the secondary dat-acenter. Therefore no regular off-site backup is necessary for the information that is stored inside the database. A full backup of the data is performed twice a week and differential (level) backup is performed daily. • The file system backup of the database server is performed once a week and daily (differential).These backups are performed as a local backup to tape. • All backups are subject to retention with requirements aligned to compliance, business and legal requirements. • All backup tapes are stored for a preselected time period (retention time) ac-cording to company policy. • Appliances and servers using VMWare are backed up by taking a snapshot of the system. • Readiness Tests on Data Back-up and Recovery are performed every six months. In addition, tests are performed after every change of the backup infrastructure and of the backup environment. • Wirecard plans business continuity and IT disaster management based on the general Risk Management, IT Risk Management process and underlying Busi-ness Impact Analysis. The general concept of the infrastructure setup and the online processing systems adheres to a high-availability and high-resilience set-up through clustering and redundancy mechanisms both on hardware as well as on application level.

Process for regularly testing, assessing and evaluating the effective-ness of technical and organizational measures (Art. 32 (1) d) GDPR)	• Parts of Wirecard are subject to BaFin audit at least annually. • Wirecard is a PCI DSS compliant company and is assessed annually by Qualified Security Assessors (QSA) against PCI DSS requirements. • Wirecard systems undergo vulnerability assessments at least quarterly which are conducted by Internal Security Analysts. The scans are performed against all of our production solutions to ensure effective review of known risks. • External vulnerability assessments are conducted by an Approved Scanning Vendor (ASV) quarterly, to ensure our external facing solutions remain compliant with PCI DSS requirements; these scans are conducted through our PCI auditing company. • Penetration tests on network layer and application layer are performed at least annually on Wirecard systems or on significant changes. Tests are performed from internal and external. • In addition to the tests mentioned above, scans for unauthorized wireless access points are conducted at least quarterly. This process is to be carried out by a trained individual within the IT Security team. The scan is performed at all loca-tions including datacenters and office premises.