Computop Terms and Conditions

1. About This Agreement and the Services

1.1 This Agreement (comprising the Order Form(s), these Terms and Conditions and the associated Data Processing Agreement) sets out the terms and conditions for the provision of the Services by Computop Wirtschaftsinformatik GmbH on behalf of Computop Limited ("Computop") to you, the individual or organization which enters into the Order Form(s) with Computop for the Services.

1.2 The Services provide a payment gateway which communicates with the relevant parties to a Transaction. For example, Computop captures the payment details provided by Company's Customers, which Computop sends to Company's Acquirer. Company's Acquirer sends the details to the Customer's payment card issuer which authorises or declines the Transaction. Company's Acquirer then sends the Transaction results back to Computop and Computop sends the results to Company to relay the results of the Transaction.

2. Definitions

2.1 "Acquirer" means a regulated third party bank or financial institution which has an agreement with the Company to process the payment instructions received from a Customer by Computop's intermediation via the Computop Paygate for the payment method selected by the Customer. Following Authorisation, the Acquirer acquires the relevant Transactions and effects payment of the purchase price (and "Acquiring" shall be construed accordingly). For the avoidance of doubt Computop is not the Acquirer.

2.2 "Agreement" means collectively, these Terms and Conditions, together with each Order Form and all attachments, exhibits, schedules, policies, and instructions incorporated by reference thereto.

2.3 "Alternative Payment Provider" means a provider of a payment method which can be used by the Company as an alternative to a card payment (i.e. credit, debit, charge, purchase or other card payment). For the avoidance of doubt Computop is not an Alternative Payment Provider.

2.4 "Authorisation" means the status indicating that the Acquirer or Alternative Payment Provider has validated the Authorisation Request and (in case of a card-related Transaction) has reserved the amount and has deducted it from the cardholder's spending limit.

2.5 "Authorisation Request" means the submission by the Company to the relevant Acquirer or Alternative Payment Provider via the Computop Paygate of Transaction data for the purposes of validating a payment in respect of a Transaction.

2.6 "Capture Request" means the submission by the Company to the relevant Acquirer or Alternative Payment Provider via the Computop Paygate of Transaction data after receipt of an Authorisation for the purposes of executing a payment instruction in respect of a Transaction.

2.7 "Company" means the entity identified as such on the first page of the Order Form.

2.8 "Company Data" means information submitted by, or entered by a Customer or prospective Customer through a Company Website, including, but not limited to, account information, credit card information, bank account information, accounting information, transactions and reports.

2.9 "Computop Paygate" means the processing of Authorisation Requests and Capture Requests on the System on behalf of Company over the internet.

2.10 "Confidential Information" means any and all information disclosed by either party (the "Disclosing Party") to the other (the "Receiving Party"), which is marked "confidential" or "proprietary" or which should reasonably be understood by the Receiving Party to be confidential or proprietary, including, but not limited to, the terms and conditions of this Agreement, the Company Data, and any information that relates to business plans, services, marketing or finances, research, product plans, products, developments, inventions, processes, designs, drawings, engineering, formulae, markets, software (including source and object code), hardware configuration, computer programs, and algorithms of the Disclosing Party.

2.11 "Customer" means an individual, company or other entity who has ordered goods and/or services from the Company via a Company Website and who has initiated a Transaction in respect of that order and where payment for such order is to be processed using the Services.

2.12 "Data Processing Agreement" means an agreement between the parties in the form set out in Schedule 1 to this Agreement.

2.13 "Documentation" means the written instructions or manuals, including any updates thereto, relating to the use of the Services as published by Computop or otherwise made available to its customers generally.

2.14 "Error" means the failure of the Services on the System to substantially conform to the Documentation.

2.15 "Intellectual Property" means any intellectual property or proprietary rights, including but not limited to copyright rights, moral rights, database rights, trademarks (including logos, slogans, trade names, service marks), patent rights (including patent applications and disclosures), know-how, inventions, rights of priority, and trade secret rights, recognised in any country or jurisdiction in the world.

2.16 "Order Form" means an order form for Services which is signed by (and therefore contracting binding on) both parties and which is part of the Agreement between the parties.

2.17 "Services" means the Computop Paygate and such other services and products specified in the applicable Order Form(s) (as more particularly described in the Documentation). Except where expressly stated otherwise in an Order Form, the Services do not include any payment services as defined in the Payment Services Regulations 2009.

2.18 "System" means the software and hardware used by Computop to provide the Services, including application software, Web and/or other Internet servers, any associated offline components, and all updates thereto.

2.19 "Term" means the term of this Agreement as set out in section 10.1 and the applicable Order Form.

2.20 "Transaction" means any transaction between the Company and a Customer via a Company Website in relation to which the Services are supplied.

2.21 "Website" means the merchant website(s) specified in the Order Form.

3. Computop Services

3.1 Computop shall provide the Services set out in the Order Form during the Term.

3.2 Computop shall ensure that the Computop Paygate is provided by Computop Wirtschaftsinformatik GmbH.

3.3 During the Term, Computop grants to Company a non-exclusive, non-transferable licence (with no right to grant sublicences) to access and use relevant Documentation and to use the Services selected on the Order Form(s) at the price agreed upon in such Order Forms for the purpose of facilitating Transactions.

3.4 If Company requires Computop to provide professional services in relation to configuring Company's systems for any reason, such professional services shall be set out in an Order Form for the same. If Computop agrees to render such services in relation to the Company's system, Company bears the costs incurred in accordance with the applicable Order Form, or if such Order Form is silent as to such costs, then at Computop's then current pricing.

3.5 Computop is entitled to use third parties or subcontractors to render any of the services hereunder. Company acknowledges that Computop Wirtschaftsinformatik GmbH provides the Computop Paygate and certain other Services on behalf of Computop Limited acting as its subcontractor.

3.6 The parties acknowledge that Computop only acts as technical service provider between the Company and the financial institutions regarding the handling of the Transactions.

3.7 Computop will provide the Services with reasonable skill and care and in accordance with good industry practice.

3.8 Computop shall be entitled to change the Services from time to time (including disconnecting redundant payment methods) where reasonably necessary. Computop shall give reasonable prior written notice of material changes to Company where reasonably practicable.

4. Obligations of Company

4.1 Company is responsible for the programming and linking of Company's Website(s), shop or any other system used by the Company, to the Services.

4.2 In certain circumstances Company's use of particular Computop Services may require Company to engage third parties to provide development or other services. In such circumstances Computop may provide details of third party service providers for Company to consider, but by doing so Computop does not make any recommendation or endorsement of third party service providers and Company shall be solely responsible for assessing their suitability. Accordingly, Computop does not accept any responsibility or liability for the performance of such service providers.

4.3 Company shall: (a) provide all details required by the Documentation for the acceptance and effecting payment processing via the Computop Paygate or to impart them on demand; (b) transfer all data in their correct and processible form; (c) notify Computop in writing of all changes to Company information set out in the Order Form without delay; (d) document and impart to Computop all disruptions, defects or other drawbacks relating to the Services together with a sufficiently detailed description including effects; and (e) settle all complaints from Customers without delay.

4.4 As between Company and Computop, Company shall be responsible for the settlement of the Transaction payments. Computop does not calculate the Transaction amounts or approve, issue, receive, possess or manage any payments or money.

5. Fees and Payments

5.1 Fees. The fees applicable to this Agreement will be stated in the applicable Order Form. Computop reserves the right to change fees or to institute new fees at any time. Company will be notified in advance of the effective date of changes in fees or new fees via electronic mail. Such changes or new fees will become effective upon the later of Company's next billing cycle or thirty (30) days from the date of notice ("Change Date") provided that if such changes or new fees result in an increase to the fees for the Services exceeding 5% in any 12 month period during the Term then Company shall be entitled to terminate this Agreement for convenience on prior written notice to Computop effective on the Change Date.

5.2 Payment and Reporting. Company agrees to pay the fees in the amounts and under the terms set forth in the Order Form. Company agrees to provide Computop with, and maintain accurate Company information, including, without limitation, Company legal name, address, telephone number, email address, and a valid bank account with sufficient funds for automatic charges by Computop. Failure to maintain this information may, at Computop's option, result in suspension or termination of Company's right to use the Services.

5.3 Billing. For recurring monthly fees, Computop will charge Company's bank account at the beginning of each billing period for all fees then due and any applicable taxes on such amounts. For transaction fees, Computop will charge Company's bank account at the end of each billing period for all transaction fees then due and any applicable taxes on such amounts. In the event that funds are unavailable from Company's account and Company's account is ten (10) days or more overdue, in addition to any of its other rights or remedies, Computop reserves the right to terminate the applicable Order Form, this Agreement and/or access to the Services. Any late payments will accrue late charges at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower.

5.4 Third Party Fees and Costs. Company is responsible for all third party expenses and charges associated with accessing the Services.

5.5 Taxes. All fees listed in the Order Form(s) are exclusive of any taxes, including without limitation, sales, use, excise, value-added taxes, or any other taxes based on this Agreement, or the use of the Services (collectively, the "Taxes"). Company will be responsible for all Taxes, excluding taxes based on Computop's net income.

6. Proprietary Rights

6.1 Ownership. As between Computop and Company, Computop owns or licenses all rights, including Intellectual Property rights, in the Services and System, any materials relating thereto, and any modifications, enhancements, customisations, updates, revisions or derivative works thereof, and all results of consulting services, whether made pursuant to this Agreement or otherwise. No transfer of ownership will occur under this Agreement. All rights not expressly granted to Company are reserved by Computop.

6.2 As between Computop and Company, Company shall own all rights, including Intellectual Property rights, in the Company Data.

7. Confidentiality and Security

7.1 Confidential Information. Each party ("Receiving Party") hereby agrees that it will not use or disclose any Confidential Information received from the other party ("Disclosing Party") (whether directly or indirectly through a third party) other than as expressly permitted under the terms of the Agreement or as expressly authorised in writing by the Disclosing Party. The Receiving Party will use the same degree of care to protect the Disclosing Party's Confidential Information as it uses to protect its own confidential information, but in no circumstances less than reasonable care. The Receiving Party will not disclose the Disclosing Party's Confidential Information to any person or entity other than its officers, principals, employees and subcontractors who need access to such Confidential Information in order to effect the intent of the Agreement and who are bound by confidentiality terms no less restrictive than those in the Agreement.

7.2 Exceptions. The restrictions set forth in Section 7.1 will not apply to any Confidential Information that the Receiving Party can demonstrate: (a) was known to it prior to its disclosure by the Disclosing Party; (b) is or becomes publicly known through no wrongful act of the Receiving Party; (c) has been rightfully received from a third party authorised to make such disclosure without restriction; (d) is independently developed by the Receiving Party; (e) has been approved for release by the Disclosing Party's prior written authorisation; or (f) has been disclosed by court order or as otherwise required by law, provided that the Receiving Party provides prompt advance notice thereof, to the extent practicable, to enable the Disclosing Party to seek a protective order or otherwise prevent such disclosure.

7.3 Injunctive Relief. The parties agree that a breach of Section 7.1 may cause irreparable damage which money cannot satisfactorily remedy and therefore, the parties agree that in addition to any other remedies available at law or hereunder, the Disclosing Party will be entitled to seek injunctive relief for any threatened or actual disclosure by the Receiving Party.

7.4 Security. While Transaction data and/or Company Data is in Computop's possession, Computop shall protect such data by securing it to the standards required under PCI-DSS. Company acknowledges that the Internet is an open system and Computop cannot and does not warrant or guarantee that third parties cannot or will not intercept or modify Company Data or Transaction data during transmission or when such data is not in Computop's possession and that in such circumstances it is Company's responsibility to ensure that such data is protected.

7.5 Passwords. As part of the registration process, Company will set passwords in order to access the Services. Company is responsible for maintaining the confidentiality of such passwords, and Company agrees that Computop has no liability with regard to the use of such passwords by third parties. Company agrees to notify Computop immediately if Company has any reason to believe that the security of Company's account or any Customer's account has been compromised and in these circumstances Computop shall render the account inaccessible and provide a new account and passwords to Company, subject to Computop's published set-up fees applicable for such changes and new configuration.

8. Personal Data

8.1 Each party acknowledges that Company Data may include personal data, the processing of which must be governed by a Data Processing Agreement in the form set out at Schedule 1.

9. Availability

9.1 Availability. Computop uses commercially reasonable efforts to maintain monthly availability of the Computop Paygate at 99%, subject to the exceptions set forth in Sections 9.2 and 9.3 ("Monthly Availability"). If Computop is unable to meet this Monthly Availability level for the Services in any month, Computop will provide to Company a credit equal to half the monthly recurring fee paid by Company for such month. In order to receive a credit Company must submit a request for credit to Computop within fifteen (15) days after the month in which the availability failure occurred. Any credit will be applied against subsequent monthly fees due to Computop. In the event Computop fails to achieve the Monthly Availability level set forth in this Section 9.1 solely through its own fault for two (2) consecutive months or by more than three times in a twelve (12) month period, Company shall have the right to request in writing that Computop produce the Monthly Availability in accordance with this Section 9.1. Thereafter, should Computop fail to meet the Monthly Availability once more within the six (6) months following the Company's written request, Company shall have a right to terminate this Agreement upon written notice to Computop. This Section 9.1 states Company's exclusive remedy, and Computop's entire liability, for the failure to meet Monthly Availability levels.

9.2 Exceptions; Downtime. Scheduled and unscheduled interruptions may occur, and Computop does not warrant uninterrupted availability of the System or the Services. Excluded from the Monthly Availability calculation are: (a) scheduled software or hardware maintenance, (b) downtime due to force majeure issues; or (c) any issues caused by Company. Normal software or hardware maintenance are scheduled for nights and weekends, and designed to cause a minimum amount of interruption to Services and System availability. Company will be notified of scheduled interruptions in advance. In the event that an unscheduled interruption occurs, Computop will use commercially reasonable efforts to resolve the problem and return the Services to availability as soon as practical. During these scheduled and unscheduled interruptions, Company may be unable to transmit and receive data through the Services. Company agrees to cooperate with Computop during the scheduled and unscheduled interruptions if assistance from Company is necessary in order to restore the System and Services to working order.

9.3 Suspension. Computop reserves the right to temporarily suspend use of the Services or portions thereof in its reasonable discretion, including but not limited to the following circumstances: (a) Computop is required to suspend the Service(s) under card or payment scheme rules; (b) Computop is required to suspend the Services by an order of a court or regulatory authority; (c) Computop reasonably suspects Company of breach of the Agreement; (d) Computop suspects the occurrence or likely occurrence of fraud or a security breach affecting the Transaction, Computop's System or the Services. Computop may also impose temporary limits on certain features and services or temporarily restrict Company's access to parts of the Services for maintenance or system administration purposes without notice or liability. Where reasonably practicable, Computop shall give reasonable prior written notice of any such suspension to Company and Computop shall endeavor to minimize the duration of any suspension or restriction.

10. Term and Termination

10.1 Term. Unless expressly stated otherwise in the applicable Order Form, the initial term of this Agreement and any Order Form hereunder will be three (3) years from the execution date of the initial Order Form, and will automatically renew for successive one (1) year periods (each from the anniversary date of either the execution date of the initial Order Form or the execution date the most recent of any subsequent Order Form if later) unless one party notifies the other party that it does not wish to renew this Agreement

at least ninety (90) days prior to the end of the then-current term. In addition, Computop shall have the right to terminate this Agreement, in whole or in part, at any time on ninety (90) days' notice, in the event certain of its Services (such as giropay) can no longer be offered by Computop.

10.2 Termination for Cause. Either party may terminate this Agreement and/or the affected Order Form for cause upon thirty (30) days written notice of a material breach to the other party if such breach remains uncured at the expiration of such period. In addition, Computop may terminate this Agreement immediately for any failure of Company to pay amounts due by it that are ten (10) days or more past the due date.

10.3 Effect of Termination. Termination will not relieve Company of the obligation to pay any fees due or payable to Computop prior to the effective date of termination, or any other fees or payments that Company has committed to under the Agreement. Sections 6, 11.3, 12, 13 and 15 will survive any termination or expiration of the Agreement. Sections 7.1-7.3 will survive for three (3) years after termination of the Agreement.

10.4 Return of Materials. All Confidential Information, designs, drawings, formulas or other data, financial information, business plans, literature, and sales aids of every kind will remain the property of the Disclosing Party. No later than thirty (30) days after termination, each party will prepare all such items in its possession for shipment to the other at the Disclosing Party's expense. The Receiving Party will not make or retain any copies of any Confidential Information other than a single copy of the Confidential Information to the extent necessary for it to comply with applicable laws, regulations and card scheme requirements provided always that Section 7 shall continue to apply to such copy while it remains in the Receiving Party's possession or control.

11. Warranties

11.1 Warranty. Computop warrants that the Services will function substantially in conformance with the Documentation.

11.2 Notices and Correction of Errors. Company will notify Computop in writing of any Errors. Computop will use commercially reasonable efforts, at its own expense, to determine if there is an Error, and to correct or remedy Errors within a reasonable period of time following receipt of such notice. Company will make reasonably appropriate adjustments to mitigate adverse effects of any Error until Computop corrects or remedies such Error.

11.3 DISCLAIMER OF WARRANTIES. EXCEPT AS EXPRESSLY PROVIDED IN SECTION 11.1 ABOVE, COMPUTOP DISCLAIMS ALL WARRANTIES WITH RESPECT TO THE SERVICES, SYSTEM, AND DOCUMENTATION, WHETHER EXPRESS OR IMPLIED BY LAW, REPRESENTATION STATEMENTS, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. EACH PARTY WILL BE SOLELY AND INDIVIDUALLY RESPONSIBLE FOR COMPLYING WITH ALL LAWS AND REGULATIONS RELATING TO ITS RESPECTIVE BUSINESS OPERATIONS.

11.4 Remedies. For any breach of the warranties contained in Section 11.1 above, Company's exclusive remedy, and Computop's entire liability, shall be the correction of Errors that caused the breach of the warranty, or if Computop is unable to make the Services operate as warranted, Company shall be entitled to terminate this Agreement.

12. Indemnification

12.1 Computop Indemnification. Computop agrees to indemnify Company against any losses or damages finally awarded against Company incurred in connection with a third party claim alleging that the Company's use of the unaltered Services infringes or misappropriates any patent, copyright, or trade secret of such third party, provided that Company: (a) provides prompt written notice of such claim to Computop and in any event no later than two (2) business days after Company becomes aware of the claim, (b) grants Computop the sole right to defend or settle such claim, (c) does not make any admissions or otherwise compromise the defense of such claim and (d) provides to Computop all reasonable assistance. In the event of a claim or threatened claim under this Section 12.1 by a third party, Computop may, at its sole option, (i) revise the Services so that they are no longer infringing, (ii) obtain the right for Company to continue using the Services and System, or (iii), terminate the Agreement upon ten (10) days written notice. THIS SECTION 12.1 REPRESENTS THE SOLE AND EXCLUSIVE LIABILITY OF COMPUTOP AND THE EXCLUSIVE REMEDY OF COMPANY FOR INFRINGEMENT OR MISAPPROPRIATION OF THIRD PARTY RIGHTS.

12.2 Indemnification by Company. Company will defend, indemnify and hold Computop harmless against any loss or damage incurred in connection with a third party claim arising from: (i) any allegation that Company Data or the collection or use thereof by Computop or Company, infringes or misappropriates any third party right, (ii) a claim related to Company's modifications or misrepresentation of the Services, or (iii) a claim by any Customer, former customer or service provider of Company; provided, that Computop (a) provides prompt written notice of such claim to Company, (b) grants Company the sole right to defend or settle such claim, (c) does not make any admissions or otherwise compromise the defense of such claim, and (d) provides to Company all reasonable assistance.

13. Limitation of Liability

13.1 Nothing in this Agreement shall limit each party's liability for its fraud or for death or personal injury resulting from the negligence of its employees.

13.2 Except as set out in Section 12, neither party will be liable under this Agreement for indirect or consequential loss.

13.3 Without prejudice to the generality of Section 13.2, Computop is not liable to Company for any losses or damages (including penalties) arising from (i) Company's failure to comply with Section 15.6, or (ii) any third party's failure to comply with the Payment Services Regulation 2009, the Electronic Money Regulations 2011, anti-money laundering and counter terrorist financing laws, or equivalent local or European legislation.

13.4 Computop's total aggregate liability under this Agreement (regardless of the form of action and whether in contract or tort or otherwise) in any 12 month period shall be limited to either £10,000 or 125% of the fees paid by Company during that 12 month period, whichever is greater.

14. Publicity

14.1 Each party may identify the other party (a) on websites or in sales presentations or marketing materials provided that such website, lists or materials list only the party by name and/or logo and state generally the relationship between the parties, or (b) in disclosures to the extent required to meet legal or regulatory requirements.

15. General Provisions

15.1 Notices. Except as otherwise specified in the Agreement, all notices under the Agreement will be in writing and will be delivered or sent by (a) registered or otherwise recorded mail; or (b) a courier with a tracking system, to the address specified in the applicable Order Form; or (c) email to the address specified in the applicable

Order Form provided all legal notices regarding breach or termination must be sent to the relevant party recipient by hand, pre-paid post or courier. Notices will be deemed to be received when signed for according to relevant postal or courier procedure or in the case of email, at the time the email is delivered to the recipient's email server (evidenced by a delivery receipt). Either party may change its address by giving timely notice of the new address to the other party pursuant to this Section and identifying in such notice the date on which such change is effective.

15.2 Independent Contractors. The relationship of Computop and Company is that of independent contractors. Neither party has any authority to act on behalf of the other party or to bind it, and in no event will the parties be construed to be partners, employers, employees, or agents of each other.

15.3 Governing Law. This Agreement shall be governed by English law and the parties irrevocably submit to the exclusive jurisdiction of the English courts in relation to any dispute arising in connection with this Agreement.

15.4 Assignment. The Agreement may not be assigned, transferred, sub-contracted or otherwise disposed of, in whole or in part by Company, without the prior written consent of the Computop.

15.5 Force Majeure. Notwithstanding any provision contained in the Agreement, neither party will be liable to the other to the extent fulfillment or performance of any terms or provisions of the Agreement are delayed or prevented by revolution or other civil disorders; wars; strikes; labour disputes; electrical equipment or availability failure; fires; floods; acts of God; government action; or, without limiting the foregoing, any other causes not within its control and which, by the exercise of reasonable diligence, it is unable to prevent. This Section will not apply to the payment of any sums due under the Agreement by either party to the other.

15.6 Compliance With Laws. Company undertakes to comply with all applicable laws and to obtain and maintain all necessary consents or authorisations (whether governmental/regulatory or otherwise) in order to utilise the Services.

15.7 Miscellaneous. Headings in the Agreement are for reference purposes only and will not affect the interpretation or meaning of the Agreement. If any provision of the Agreement is held by an arbitrator or a court of competent jurisdiction to be contrary to law, then the remaining provisions of the Agreement will remain in full force and effect. No delay or omission by either party to exercise any right or power it has under the Agreement will be construed as a waiver of such right or power. A waiver by either party of any breach by the other party will not be construed to be a waiver of any succeeding breach or any other covenant by the other party. All waivers must be in writing and signed by the party waiving its rights. No Section of the Agreement is intended for the benefit of any third party, and the parties do not intend that any Section of the Agreement should be enforceable by a third party either under the Contracts (Rights of Third Parties) Act 1999 or otherwise.

15.8 Entire Agreement. The Agreement constitutes the entire agreement between Computop and Company with respect to the subject matter hereof. The Agreement supersedes all prior negotiations, agreements, and undertakings between the parties with respect to such subject matter and each party agrees that it has not entered this Agreement relying on any non-fraudulent statement which is not expressed in this Agreement. No modification of the Agreement will be effective unless contained in writing and signed by an authorised representative of each party. Additional Order Forms may be added to the Agreement by reference to these Terms and Conditions, provided that each such Order Form is signed by both parties. No term or condition contained in Company's purchase order or similar document will apply unless specifically agreed to by Computop in writing, even if Computop has accepted the order set forth in such purchase order, and all such terms or conditions are otherwise hereby expressly rejected by Computop.

15.9 Order of Precedence. In the event of any conflict or ambiguity between the documents comprising the Agreement, the conflict or ambiguity shall be resolved according to the following descending order of precedence: (a) the Data Processing Agreement (regarding any matter relating to personal data; (b) these Terms and Conditions; and (c) the Order Form(s) (with the most recent taking precedent over any prior Order Forms).

Schedule 1

FORM OF DATA AGREEMENT

DATA PROCESSING AGREEMENT

between

Name of the company
Address
Address

- hereinafter Controller–

and

Computop Ltd.
3000 Hillswood Business Park
Hillswood Drive
Chertsey, Surrey KT16 0RS
United Kingdom

- hereinafter Processor –

PREAMBLE

This data processing agreement shall specify the parties' rights and obligations associated with the processing of personal data. In particular, it shall govern the legally required contract contents in accordance with Article 28 of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR).

The definitions of the GDPR shall apply.

This agreement shall apply as a framework agreement to all existing contractual agreements between the parties under which the Processor processes personal data on the Controller's behalf. This shall include, in particular, all existing orders for the installation Paygate as well as all other contracts or framework contracts including associated individual contracts between the parties whose subject is the processing of personal data by the Processor. These contractual agreements shall hereinafter be called „main contract" or „main contracts".

The agreement shall also apply if the Controller is an authorised partner who resells the Processor's services. In the latter cases, this agreement shall solely be concluded between the authorised partner and the Processor. The authorised partner shall thereupon himself be obliged to conclude comparable data processing agreements with his customer companies.

The same shall apply if the main contract between Processor and Controller authorises affiliated companies of the Controller who are not a party to the main contract, including in particular to a framework contract or associated individual contracts, to make use of the services of the Processor. In these cases, the Controller shall himself be obliged to conclude comparable data processing agreements with his affiliated companies.

The general principle shall be that only a party which is a party to the main contract with the Processor may become a party to this data processing agreement

1. SUBJECT-MATTER AND DURATION OF THE PROCESSING

- Article 28 section 3 sentence 1 GDPR –

Subject-matter and duration of the processing are specified in the respective underlying main contract. If there are several main contracts between Controller and Processor, this agreement shall apply to all of these main contracts, and in each case for the duration of the existence of the respective main contract.

2. NATURE AND PURPOSE OF THE PROCESSING, TYPE OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

- Article 28 section 3 sentence 1 GDPR –

Nature and purpose of the processing, type of personal data and categories of data subjects are specified in Appendix 1.

The Computop Paygate is hosted on a data center in Germany. The Processor shall be entitled to move abroad the data processing of single components which do not involve the direct reception of payment orders and execution of payment transactions in the Paygate. This shall apply, in particular, when ordering products where it is pointed out that Sub-Processors are used which are based abroad. Provided, it is ordered accordingly by the Controller, data processing abroad shall be permitted e.g. in the area of fraud prevention. Moving data processing to states outside the European Union or the European Economic Area shall only be permissible if the requirements prescribed in Article 44 et seq. GDPR are fulfilled.

3. TECHNICAL AND ORGANISATIONAL MEASURES

- Article 28 section 3 sentence 2 lit. c) in conjunction with Article 32 GDPR –

The Processor will take technical and organisational measures according to Article 32 GDPR which, within the course of this processing, are necessary to ensure compliance with statutory data protection provisions. Such technical and organisational measures are set out in Appendix 2.

Technical and organisational measures are subject to technical progress and further development. As a result, the Processor may deviate from the measures agreed on with the Controller and replace them with alternative adequate measures, provided these do not fall below the level of protection of the originally agreed measures.

4. OBLIGATIONS OF THE CONTROLLER TOWARDS DATA SUBJECTS

- Article 28 section 3 sentence 2 lit. e) GDPR –

The Controller shall be solely responsible for fulfilling the legal obligations towards data subjects, in particular the obligation to execute the legally required information and notification duties towards data subjects, as well as the obligation to answer and execute requests of data subjects for the exercise of their rights (hereinafter summarized as “obligations towards data subjects”), including the review of the lawfulness in this context. In addition to the information and notification duties which the Controller has to fulfill, the Controller shall have, in particular, the obligation to answer and implement the data subjects' rights of access to information, rectification, erasure, restriction, data portability, the right to object as well as the rights in connection with automated individual decision-making including profiling.

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligations towards data subjects. The Processor’s obligation to support the Controller shall only exist to the extent in which fulfilling the Controller's obligations towards data subjects is, due to the specific arrangement of the processing, not possible for the Controller, or to the extent the Controller has no access to the necessary information. In particular, this shall mean that, in order to fulfil obligations towards data subjects, the Controller has to use the information and instruments which the Processor particularly provides or makes available to him through the Computop Paygate.

The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, to fulfil his aforementioned obligations towards data subjects within a period of one month of receipt of the request, provided there are no reasons for the extension of this period after applicable law.

If, within the context of a request from a data subject, it is necessary to prove the data subject’s identity, potentially also by requesting additional information, this shall be the responsibility of the Controller.

Should a data subject directly contact the Processor with regard to a request relating to the Controller’s obligations towards data subjects, the Processor will forward this request to the Controller who will then decide how to proceed. Should it, in an individual case, become necessary that the fulfilment of obligations towards data subjects will be carried out directly be the Processor, the Processor shall only be obliged to take action if he has received a documented instruction by the Controller as set out in clause 9 of this agreement.

The Processor will only disclose information to third parties (e.g. police, prosecution, courts, supervisory authorities or other authorities) related with personal data for which the Controller is responsible as set out in the GDPR, if he receives a documented instruction by the Controller or if he himself is legally obliged to provide the respective information (e.g. in the case of a legal obligation to testify as a witness).

5. OBLIGATIONS OF THE PROCESSOR

- Article 28 section 3 sentence 2 lit. f) GDPR –

Taking into account the nature of processing and the information available, the Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR

In accordance with the aforementioned provisions, the Processor has, in particular, appointed a data protection officer (Articles 37-39 GDPR) whose contact details he will provide to the Controller upon the latter's request. Moreover, he will, for the purpose of data processing, only appoint persons who have been bound in writing to comply with the data secrecy or who have in accordance with the provisions of the GDPR been bound by confidentiality. Concerning the Controller's obligation to conduct a potentially required data protection impact assessment as well as, in this context, the potentially required obligation to consult the supervisory authority (Articles 35, 36 GDPR), the Processor will support the Controller, to the extent necessary, in compiling the information required in this context, if and in so far the relevant information is not yet already available to the Controller, e.g. through his access to the Computop Paygate.

6. SUB-CONTRACTUAL RELATIONS (OTHER PROCESSORS)

- Article 28 section 3 sentence 2 lit. d) in conjunction with sections 2-4 GDPR –

„Other processors" within the meaning of the GDPR shall hereinafter be called „Sub-Processors".

6.1 The Controller is familiar with the fact that the Processor is solely acting as a reseller of the Computop Paygate, a platform developed, hosted and operated by its parent company Computop Wirtschaftsinformatik GmbH, Schwarzenbergstraße 4, 96050 Bamberg, Germany, and the data processing is in its entirety conducted by Computop Wirtschaftsinformatik GmbH. Therefore, the Controller hereby acknowledges and agrees that the Processor uses Computop Wirtschaftsinformatik GmbH as a Sub-Processor.

6.2 The Controller hereby grants the Processor (provided he has not yet granted him a prior specific written authorisation, e.g. in the context of a purchase order in which the use of a Sub-Processor was explicitly pointed out) a general authorisation to use Sub-Processors if

- the Processor has informed the Controller of the intended use of a Sub-Processor in advance and in writing, either in an electronic form or in text form and
- the Processor imposes, by way of a contractual agreement, which is made in writing or in an electronic form, data protection obligations on the Sub-Processor which correspond with the data protection obligations of this agreement.

The obligation to inform the Controller shall also apply to each intended change concerning the involvement or replacement of Sub-Processors.

In justified cases, the Controller shall be entitled to object to the use or intended changes concerning the involvement or replacement of Sub-Processors if there is duly substantiated concern for the assumption that the new Sub-Processor cannot ensure the protection of the Controller's personal data. The objection of the Controller against the use of a Sub-Processor shall have to be raised within a period of one month, starting from the end of the month in which the Controller has received the information. After expiry of this period, any objection shall be excluded.

If the Controller objects to the use of a Sub-Processor, the Processor shall have a special termination right with regard to the corresponding part of the service. The special termination right shall have to be exercised within a period of one month, starting from the end of the month in which the objection was received. If the special termination right is exercised, the main contract(s) shall, for the corresponding part of the service, end within three months, starting from the end of the month in which the special termination right was exercised. The Processor shall not be liable for costs (including in particular costs associated with migrating to an alternative service provider), expenses or damages arising from such termination under this agreement or under the main contracts unless there is a justified case within the meaning of this clause 6.2.

6.3 The Controller shall, upon the conclusion of the contract as well as during audits in accordance with clause 7 of this agreement, have the right to request from the Processor an up-to-date list of Sub-Processors currently in use.

6.4 Sub-Processors within this specific data processing agreement shall mean such third parties who are processing personal data on behalf of the Processor as part of the Processor's performance of the Computop Paygate. Sub-Processors shall not include third parties which the Processor uses for ancillary services that are supporting the performance of the services, third parties which are performing services that are permitted by a statutory provision or third parties which are performing services directly to the Controller and therefore are in a direct contractual relationship with the Controller (e.g. banks, including acquirers, meaning the banks of the merchant which settle payments by customers via credit card, credit agencies, telecommunication service providers, postal operators, transport service providers, cleaning staff or companies used for data carrier destruction). The Processor will, nevertheless, also make appropriate contractual agreements with these third parties in order to ensure data protection and data security and will implement control measures where required by law (in particular if the respective ancillary services constitute a data processing on behalf of the Controller in the relationship between the Processor and the third party).

6.5 The Processor will audit Sub-Processors which are potentially used by him in accordance with applicable law. A direct audit right of the Controller towards Sub-Processors potentially used by the Processor shall not exist.

7. AUDIT RIGHTS OF THE CONTROLLER

- Article 28 section 3 sentence 2 lit. h) GDPR –

The Controller shall be entitled to verify the Processor's compliance with the agreed technical and organisational measures as well as with statutory obligations in connection with the data processing before the data processing begins and regularly thereafter. Moreover, he shall also be entitled to use third parties to carry out these audits.

The parties agree that during the performance of audits, the provision of the current certificate after the Data Security Standard of the Payment Card Industry (PCI-DSS) which Computop Wirtschaftsinformatik GmbH has received, and, if necessary, of the related „Attestation of Compliance", issued by an independent auditor and which contains a summary of the audit results, shall usually be sufficient. The respective current certificate can be downloaded on the website www.computop.com/uk/. The underlying audit criteria are available on the PCI Standard Council's website www.pcisecuritystandards.org. Upon request, the Controller shall also receive the respective current „Attestation of Compliance".

More extensive audits, such as, in particular, the request of further information and documents, audits through questionnaires or on-site inspections at the Processor's premises, shall only be carried out if the aforementioned documents give reasonable cause for this. The Processor shall allow for and contribute to audits. A date for the conduct of audits is to be agreed between Controller and Processor well in advance.

8. PROCESSOR'S OBLIGATION TO INFORM ABOUT VIOLATIONS

- Articles 33, 34 GDPR

The Processor is obliged to inform the Controller without delay if he becomes aware of data breaches occurring during the data processing which might lead to notification obligations towards the supervisory authority as well as to communication obligations towards data subjects. This shall apply regardless of the fact whether the data breach is based on an infringement by the Processor or persons employed by him against data protection regulations or contractual agreements, or if it is based on independent circumstances (such as an attack by third parties or force majeure). Articles 33 and 34 GDPR shall apply.

The Controller is responsible for the fulfilment of potential notification and communication obligations in the circumstances set out above. Taking into account the nature of the processing and the information available to him, the Processor will support the Controller in the fulfilment of these obligations to the extent reasonably required. The Processor's obligation to support the Controller in these circumstances is limited to providing information which the Controller needs and which are not known to him or which he does not have access to himself (e.g. through having access to the Computop Paygate).

9. EXTENT OF THE CONTROLLER'S RIGHT TO ISSUE INSTRUCTIONS

- Article 28 section 3 sentence 2 lit. a) and sentence 3, Article 29 GDPR –

It is the Controller's sole responsibility that the processing will be performed in compliance with applicable law and that the rights of the data subjects will be observed. Therefore, it is his sole responsibility to specify the framework conditions for the Processor for this purpose. The framework conditions shall be set out specifically in this agreement and the underlying main contracts. The Processor and the persons subordinated to him are only permitted to process personal data of the Controller within this framework as well as, beyond that, only based on a documented instruction by the Controller. Processing of data beyond a documented instruction shall only be permitted if the Processor is obliged to undertake such processing by the law of the European Union or the law of the member state to which he is subject.

The Controller must issue instructions to the Processor in writing or by e-mail.

The Controller's right to issue instructions shall be limited to such instructions that serve to ensure the fulfillment of legal data protection obligations which are constituted by the respective current data protection law as shaped in the provisions of this agreement, and shall only exist within the framework of the services offered by the Processor and the variants and modalities offered in this context. The Processor shall not be obliged to fulfill instructions that are going beyond that. This shall also apply if an instruction refers to taking specific technical or organisational measures. Such modifications usually require a mutual agreement between Controller and Processor by way of an extension of the main contract and with determining a corresponding fee.

Apart from that, the Controller will always have the opportunity to instruct the Processor to discontinue a particular service within a reasonable period of time depending on the circumstances. The duration of the main contract as well as the Controller's obligation of compensation shall remain unaffected by such instruction. The main contract shall continue to exist with regard to the affected service until it is terminated due to passage of time, an ordinary termination or due to a potentially existing extraordinary termination right or a special termination right.

The Processor will notify the Controller without delay if he is of the opinion that an instruction is in conflict with the applicable data protection legislation.

10. END OF PROVISION OF PROCESSING SERVICES

- Article 28 section 3 sentence 2 lit. g) GDPR

Upon the request of the Controller and no later than at the end of the provision of services relating to the processing, the Processor shall, upon a documented instruction by the Controller, either delete all personal data or return them to the Controller unless the Processor is obliged to continue to store personal data for its compliance with applicable laws or regulations or under card scheme rules.

Provided, it is not stated otherwise in the underlying main contract and the Controller does not give a separate documented instruction to the Processor in this regard, the following shall apply: During the term of the main contract as well as after the termination of the main contract, transaction data will be deleted in the Computop Paygate database and in Computop Analytics after 12 months. In the Computop Reporter, transaction data will be deleted after 24 months. Prior to the deletion, data will be available to the Controller for viewing, analysing and secure download. On termination of the main contract, the access rights of the Controller to the Computop Paygate will be deactivated and the Controller shall be responsible for ensuring that the Controller downloads all of the Controller's data prior to such termination.

11. LIABILITY

The Processor's liability towards the Controller regarding claims for compensation arising from a violation of data protection obligations, is set out in the following provisions. A violation of data protection obligations by the Processor shall be deemed to exist if he violates statutory obligations of data protection laws applicable to him as shaped in the provisions of this agreement as well as in documented instructions by the Controller that are legally permitted by data protection law and permitted by this agreement. The Processor shall only be liable for direct losses arising from its violation of data protection obligations as set out in this agreement, and the Processor's liability shall be subject to the limitations set out in the main contract. If Controller and Processor are, due to a joint and several liability after the provisions of the GDPR or another statutory provision on data protection which also applies to the Processor, obliged to pay compensation to a data subject or another person, the compensation between Controller and Processor in their internal relationship shall also be subject to the limitations set out in the main contract.

12. FINAL PROVISIONS

If single provisions of this agreement should be incomplete, ineffective or unenforceable, the effectiveness of the remaining provisions shall remain unaffected. In this case, the incomplete, ineffective or unenforceable provision shall be replaced by a provision which is in accordance with what the parties would have agreed on if they had known about the incompleteness, ineffectiveness or unenforceability.

Prior data processing agreements between the parties shall be entirely replaced by this agreement. Relevant data protection provisions in other parts of agreements (e.g. General Terms and Conditions) shall only have precedence over this agreement if they expand on the regulations of this agreement. If they change the meaning of the provisions of this agreement or if they remain well below the level of data protection agreed herein, they shall be superseded by this agreement.

With regard to data protection law, the law of the member state of the European Union to which the Controller is subject shall apply. Beyond that, agreements regarding the applicable law shall be made in the main contract.

Place of jurisdiction is Bamberg, Germany.

The conclusion of this agreement as well as subsequent amendments or additions must be made in writing and signed by both parties.

If, during the fulfilment of obligations from this agreement, efforts beyond the contractually agreed main services and the regular day-to-day business should arise for the Processor, in particular in the context of clauses 4, 5, 7, 8 and 9 of this agreement, Controller and Processor will agree on an additional compensation to be paid depending on the effort. In the event that the Processor, in this context, has received a documented instruction by the Controller, the Processor may refuse to carry out the instruction until he has received a confirmation by the Controller regarding the compensation in the respective particular case. In the event that an audit right according to clause 7 of this agreement shall be carried out which goes beyond the provision of the Processor's current certificate after the Data Security Standard of the Payment Card Industry (PCI-DSS) and the related „Attestation of Compliance", issued by an independent auditor, and the audit right cannot be considered as necessary as set out in clause 7 of this agreement, the Processor may refuse to the performance of the audit or to cooperation herein until the Controller has given his confirmation regarding the compensation for the audit.

Controller	Processor
_____	_____
place / date	place / date
_____	_____
signature and position	signature Computop Managing Director
_____	_____
name in capital letters	name in capital letters

APPENDIX 1 – NATURE AND PURPOSE OF THE PROCESSING, TYPE OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

1. Nature and Purpose of the processing

Depending on the provisions of the underlying main contract or the underlying main contracts, the Controller is using the Computop Paygate, a payment platform for secure payment transaction handling, developed and operated by the Processor, which the Controller provides to his customers as an authorised partner - possibly also with an own branding (so-called white label solution) or provides it – if contractually permitted – to affiliated companies for shared use.

The Computop Paygate is an interface which facilitates the technical steering of payment transactions from different channels, e.g. for payments on the internet or in online shops (e-commerce), for payments by using mobile devices such as smartphones or tablets, e.g. by way of in-app-payments (m-commerce) or for payments via POS-terminals (point-of-sale terminals, e.g. in cash desk surroundings, via mobile terminals or at machines). The Computop Paygate currently offers more than 200 national and international payment methods and acquirer connections, e.g. credit cards, debit cards, e-wallet systems (e.g. PayPal), direct debiting, online bank transfer, advance payment, purchase on account, instalment payments and much more. Furthermore, the Computop Paygate supports several fraud prevention methods.

The modules Computop Analytics and Computop Reporter are providing tools for the analysis of payments from all channels and payment methods as well as for the optimisation of turnovers (e.g. through visualised status reports, reviews and comparisons).

Computop's first-level and second-level support answers questions and solves problems in connection with the use of the Computop Paygate.

Regarding details of extent, type and purpose of the data processing, in particular regarding the scope of services and payment methods specifically ordered, reference is made to the respective main contract or the respective main contracts. Additionally, further contractually non-binding details can be found in the comprehensive documentation about the Computop Paygate, provided on the website www.computop.com.

2. Type of Personal Data

- master data and contract details of the Controller
- master data of contract partners of the Controller (e.g. system houses)
- IP addresses
- payment transaction data (e.g. credit card numbers, bank account data)
- address data
- shopping basket data (e.g. payment amount, reference number)
- steering data (e.g. Paygate parameters)

3. Categories of Data Subjects

- customers of the Controller whose payment transactions are processed in the Computop Paygate
- employees or contact persons of the Controller
- employees or contact persons of contract partners of the Controller

APPENDIX 2 – TECHNICAL AND ORGANISATIONAL MEASURES

according to Article 32 GDPR

The Processor has taken the following technical and organisational measures according to Article 32 GDPR in order to ensure the implementation of the statutory data protection provisions in the context of this processing on behalf of the Controller.

As the Processor is, moreover, also certified after the Data Security Standard of the Payment Card Industry (PCI-DSS) and in this context periodically undergoes strict external audits of its technical and organisational measures, this description will additionally in summary point out which measures are certified according to the requirements of the PCI Data Security Standard at Computop. For details, reference is made to the very extensive catalogue of assessment criteria of the PCI Data Security Standard which is available on the PCI Security Standards Council's website (https://www.pcisecuritystandards.org) in its respective current version. This catalogue of assessment criteria illustrates how comprehensive (and by far exceeding this description) the technical and organisational measures are regularly being certified at Computop.

Index

1. Pseudonymisation and Encryption

- Article 32 Section 1 lit. a) GDPR –
pseudonymisation and encryption of personal data.

1.1 Pseudonymisation

✓CERTIFIED
according to PCI-DSS,
requirement No. 3

- Article 4 lit. 5 GDPR -
Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

- **Truncation Or Masking Of Credit Card Numbers Or Bank Account Details When Being Displayed As Well As Rendering It Unreadable When Being Stored**

  The Processor is truncating or respectively masking credit card numbers or bank account details (hereinafter both summarised with the generic term Primary Account Number, PAN) whenever displayed and the full PAN is not needed. Only personnel with a legitimate business need is permitted to see the full PAN. Details about how the PAN is to be truncated or respectively masked is being determined by the PCI-DSS in its respective current version. The PAN is, furthermore, in compliance with the requirements of the PCI-DSS and the procedures determined therein, not only being made unreadable when being displayed but also when being stored – in fact in all places where it is stored. This is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 3).**

- **Pseudo Card Number (PCN)**

  In view of the above, the Controller has the option to place an order with the Processor to convert the real credit card numbers being used for payments by his customers into so-called pseudo card numbers (PCN). The latter are a pseudonomised substitute for the real credit card number which the Controller can store on his systems and use for future transactions without having to undergo an annual certification according to PCI-DSS (which would be required if he would store the real credit card number). The PCN is automatically being generated by the Computop Paygate during a payment. The last three digits of the PCN are identical to the real credit card number. The real credit card numbers will during the payment only be sent directly to the PCI-DSS certified Computop Paygate (and not to the merchant) and will be stored there. The Computop Paygate will then inform the merchant about the result of the payment by using the PCN.

- **Pseudo Bank Account Number (PBAN)**

  Likewise in view of the above, the Controller also has the option to place an order with the Processor to convert the real International Bank Account Numbers (IBAN) being used for payments by his customers into so-called pseudonomised international bank account numbers (PBAN, Pseudo Bank Account Number). The PBAN is automatically being generated by the Computop Paygate during a payment. The last three digits of the PBAN are identical to the real IBAN. The real IBANs will during the payment only be sent directly to the PCI-DSS certified Computop Paygate (and not to the merchant) and will be stored there. The Computop Paygate will then inform the merchant about the result of the payment by using the PBAN.

1.2 Encryption

✓CERTIFIED
according to PCI-DSS,
requirements No. 3 and 4,
PCI-P2PE and PCI-PIN

- **Encryption When Storing Data**

  Data Base Encryption: All data bases of the payment division are being located in an entirely encrypted area on the servers in our data center. This is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 3).**

  Hard Drive Encryption: The hard drives of the workstations (notebooks, PCs) used by the employees for data processing are being encrypted throughout the company. This is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 3).**

- **Encryption During Data Transmission**

  The transmission of personal data from the Computop Paygate via public networks (in particular between the Computop Paygate and the Controllers connected to it or between the Computop Paygate and partners, financial institutions or acquirers) is entirely being encrypted. This is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 4).**

- **Encryption At POS Terminals**

  For the handling of payment transactions via POS terminals and, in this context, the encrypted processing of payment data, the Processor is furthermore certified after the Point-to-Point Encryption Standard of the Payment Card Industry (PCI-P2PE). The Processor's respective current certificate can be obtained from the Processor's website www.computop.de. The underlying assessment criteria are available on the PCI Security Standards Council's website www.pcisecuritystandards.org.

  When processing payment transactions via POS terminals, also PIN numbers are being encrypted. In this context, the Processor complies with the PIN Security Requirements of the Payment Card Industry (PCI-PIN). This is periodically in detail being externally audited and compliance with the respective requirements is externally being confirmed.

- **Encryption Of E-Mails**

  It is possible to encrypt e-mails in case of need.

- **Using Strong Cryptography**

  It is also subject of the certification after the Data Security Standard of the Payment Card Industry that strong cryptography and security protocols are being used, only trusted keys and certificates are being accepted, the protocol in use only supports secure versions or configurations and the appropriate encryption strength is being used for the encryption methodology in use **(PCI-DSS requirement No. 4).**

- **Protection Of Cryptographic Keys/ Key Management Processes**

  Within the scope of the certification after the Data Security Standard of the Payment Card Industry, it is furthermore periodically in detail being externally audited and certified that pocedures for the protection of cryptographic keys against disclosure and misuse as well as key management processes and procedures are being implemented and documented **(PCI-DSS requirement No. 3).**

2. Confidentiality

- Article 32 Section 1 lit. b) GDPR –
Ability to ensure the ongoing confidentiality of processing systems and services.

2.1 Physical Access Control

✓CERTIFIED
according to PCI-DSS,
requirement No. 9

Measures to prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used:

- **Company Headquarters In Bamberg**

  The business premises of the Processor are being secured by an access control system which controls access to the various office corridors. The doors leading to the office corridors are being equipped with automatic door closing mechanisms and are therefore closing automatically after each opening. All employees are receiving an employee identity card with a photograph which , at the same time, serves as an access card to the office corridors (RFID). Alternatively, it is also possible to open the doors with corresponding security keys. The distribution of keys and employee identity cards is being documented in writing. Upon termination of employment, the access rights of the respective card are being blocked in the corresponding system and access to the business premises will be no longer possible. The employee identity cards and possibly handed over security keys are being returned.

  Visitors are receiving a visitors' badge and are being registered in a visitors' protocol. They are being received by an employee on the respective office corridor after ringing the bell.

  The business premises are being secured by an alarm system.

  In addition, the server room is under video surveillance.

- **Other Locations**

  Also, at all other Computop locations, adequate physical access control measures have been taken such as e.g., in particular, controlled distribution of keys, access cards or other access media.

- **Data Center**

  Computop's systems are running in two external data centers, however on Computop's own servers. The data center services are being limited to pure housing. The data centers in use are fulfilling all requirements of a proper operation of data centers. Physical access control takes place via logging access control systems, burglary and sabotage protection measures as well as video surveillance and alarm systems.

The physical access control measures of the Processor are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 9).**

2.2 General Data Processing System Access Control

✓CERTIFIED
according to PCI-DSS,
requirements No. 1, 2, 3, 6, 8, 11

Measures to prevent data processing systems from being used without authorisation:

- **User Identification**

  User identification is being realised via assigning a unique user ID to each person whereby all actions taken can be traced back clearly to the the respective initiator. The addition, deletion and modification of user IDs and credentials is being controlled. Access for any terminated users is immediately being revoked, inactive user accounts are being removed or disabled within a specified period of time. After a specified number of access attempts, the user ID will be locked out and, within a subsequent specified lockout period, only an administrator is permitted to re-enable the user ID. User IDs are not being used for groups or several persons. The

aforementioned measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 8).**

- **User Authentification**

  User authentification is being realised by using complex passwords which comply with common password policies and the PCI-requirements. Accordingly, in the systems of the Processor, a specified minimum length, the use of several character categories and a periodic change of passwords is being predetermined, while the changed passwords have to differ from a fixed number of previously used passwords. Passwords must immediately be changed after the first use. Moreover, passwords are only being transmitted and stored by using strong cryptography. Prior to performing password resets, the user identity is being verified following a predetermined procedure. The aforementioned measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 8).**

  Before installing a system on the network, the Processor changes all default passwords and removes unnecessary default accounts **(PCI-DSS requirement No. 2).**

  Authentification data necessary for payment transactions (e.g. card verification code or PIN number) are solely being used for authorisation and are not being stored **(PCI-DSS requirement No. 3).**

- **Locking Workstations**

  The employees are required to lock their workstations during absence. After a specified period of inactivity, the systems are automatically being locked so that users have to re-authenticate **(PCI-DSS requirement No. 8).**

- **Hard Drive Encryption**

  The hard drives of the workstations (notebooks, PCs) used by the employees for data processing are being encrypted throughout the company (**PCI-DSS requirement No. 3).**

- **Data Base Encryption**

  All data bases of the payment division are being located in an entirely encrypted area on the servers in our data center **(PCI-DSS requirement No. 3).**

- **Firewall Systems, Demilitarised Zone (DMZ)**

  The Processor has implemented a firewall configuration respectively a demilitarised zone (DMZ) and is maintaining it periodically. The firewall configuration has been built up according to a standard defined for this purpose, is restricting inbound and outbound traffic between the company internal network and other networks (untrusted networks, internet, etc.) to that which is necessary and specifically denies all other traffic. In addition to the server configuration, firewalls have also been installed on all workstations and mobile devices. The aforementioned measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 1).**

  Furthermore, the Processor has installed a web-application firewall that detects and prevents web-based attacks **(PCI-DSS requirement No. 6).**

- **Periodical Vulnerability Scans And Penetration Tests As Well As Use of Intrusion Detection and Intrusion Prevention Systems (IDS/IPS)**

  The Processor is periodically performing vulnerability scans as well as penetration tests from both inside and outside the network and corrects the possibly found exploitable vulnerabilities. Moreover, the Processor uses intrusion-detection and/or intrusion-prevention techniques which are giving an alert in case of suspected compromises (Intrusion Detection and Intrusion Prevention Systems, IDS/IPS). The aforementioned measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 11).**

2.3 Differenciated Data Processing System Access Control

✓CERTIFIED
according to PCI-DSS,
requirements No. 3, 7, 10

Measures to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage:

- **Roles and Rights Concept, Need-To-Know Principle**

  A roles and rights concept has been defined. Access rights are being restricted according to job responsibilities and need to know to the the least amount needed to perform the job (assignment of minimal access rights after the need-to-know principle). These access control measures by the Processor are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 7).**

- **Data Minimisation**

  The Processor is complying with the data minimisation principle.

  In particular, the storage of card holder data is being restricted to a minimum so that card holder data is only being stored as long as necessary. Moreover, the Processor has implemented policies and procedures for data retention and deletion (deletion periods and procedures for the deletion of data). This is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 3)**.

  Apart from card payments, the Controller has the option to have numerous other payment methods technically being steered by the Processor, and use various other services. With some payment methods, it is possible to transfer more data to the Processor than absolutely necessary for the steering of payment methods and services. In this context, the Controller as the responsible entity in respect of data protection, is obliged to examine himself which categories of data are specifically necessary for his intended purposes in oder to comply with the data minimisation principle.

- **Logging Systems And Evaluation Systems For Logs**

  The Processor is using logging systems and evaluation systems for logs compliant with the requirements of the PCI Data Security Standard **(PCI-DSS requirement No. 10).** Details are being outlined in section „Input Control".

2.4 Separation Control

✓CERTIFIED
according to PCI-DSS,
requirements No. 6 and 7

Measures to ensure that data collected for different purposes can be processed separately.

- **Multi-Client Capability**

  The systems of the Processor, in particular the Computop Paygate, are multi-client capable and, accordingly, have several clients.

- **Separation Via Roles And Rights Concept**

  Separation control additionaly takes place via the Processor's roles and rights concept as outlined in section "Differenciated Data Processing System Access Control". The roles and rights concept is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 7).**

- **Functional Separation Of Production And Testing Environment**

  The Processor is separating development and testing environments from the production environment. This is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 6).**

3. Integrity

- Article 32 Section 1 lit. b) GDPR -
Ability to ensure the ongoing integrity of processing systems and services;

3.1 Tranmission Control

✓CERTIFIED
according to PCI-DSS,
requirements No. 3, 4, 9, 10,
PCI-P2PE, PCI-PIN

Measures to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

- **Encryption**

  The use of encryption methods by the Processor is outlined in detail in section „Encryption". These measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirements No. 3 and 4)**, the Point-to-Point Encryption Standard of the Payment Card Industry **(PCI-P2PE)** and the PIN Security Requirements of the Payment Card Industry **(PCI-PIN).**

- **Tunnel Connection (Virtual Private Network - VPN)**

  Moreover, the Processor is using tunnel connections (Virtual Private Network – VPN).

- **Secure Data Deletion And Data Destruction**

  As soon as personal data, in whatever form (in particular data on paper or electronic data) is no longer needed, the Processor is destroying it in a way by which reconstruction will be made impossible (use of data destruction containers, shredders and methods for secure deletion of electronic data). This measure is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 9).**

- **Control Of Internal And External Distribution Of Media**

  In compliance with the requirements of the Data Security Standard of the Payment Card Industry, the Processor maintains strict control over the internal or external distribution of any kind of media and is classifying media in correspondence with the sensitivity of the data. Moreover, inventory logs of all media are being maintained. This measure is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 9).**

- **Protecting Devices Against Tampering And Substitution**

  In compliance with the requirements of the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 9)**, the Processor maintains an up-to-date list of devices which contains the information determined by the PCI-DSS for unique identification of devices, and has implemented the measures determined by the PCI-DSS for protecting devices against tampering and substitution.

3.2 Input Control

✓CERTIFIED
according to PCI-DSS,
requirement No. 10

Measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

- **Logging Systems And Evaluation Systems For Logs**

  Within the certification after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 10)**, it is periodically in detail being externally audited and certified that logging systems (audit trails) and evaluation systems for logs compliant with the requirements

therein are being used. Audit Trails serve to track all access to system components by individual users or respectively user activities in order to be able to prevent or detect data compromises and to identify the root causes of problems. In this context, it is also being audited and certified that audit trails are being secured against alteration, and that access is limited to persons with a job-related need. It is being audited and certified that logs and system events are regularly being reviewed in order to identify anomalies or suspicious activity, and that exceptions and anomalies identified during the review process are being followed-up.

- **Deployment Of Change-Detection Mechanisms For Unauthorised Modifications Of Critical System Files, Configuration Files, Or Content Files.**

  In compliance with the requirements of the Data Security Standard of the Payment Card Industry, the Processor is deploying change-detection mechanisms which are giving an alert in case of unauthorised modifications (including changes, additions, and deletions) of critical system files, configuration files, or content files. Moreover, the Processor has implemented a process in order to respond to any such alerts. The aforementioned measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 11).**

4. Availability, Resilience and Restorability

- Article 32 Section 1 lit. b) GDPR -
Ability to ensure the ongoing availability and resilience of processing systems and services.

- Article 32 Section 1 lit. c) GDPR –
Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Availability Control

✓CERTIFIED
according to PCI-DSS,
requirements No. 1, 2, 5, 6, 9, 11, 12

Measures to ensure that personal data are protected from accidental destruction or loss.

- **Backup**

  In compliance with the requirements of the Data Security Standard of the Payment Card Industry, backup procedures have been implemented, and the storage of media backups complies with the requirements laid down therein. This measure is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 9).**

- **Anti-Virus Software**

  All workstations and servers have been equipped with anti-virus software which is periodicly automatically being updated. The anti-virus software is capable of detecting, removing, and protecting against all known types of malicious software, is at all times being kept current and periodic scans are being performed. Audit logs are being generated which are being retained in accordance with the PCI-DSS requirements. The anti-virus software is actively running and cannot be disabled or altered by users. The protection of all systems against malware respectively the use of anti-virus software is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 5).**

- **Firewall Systems, Demilitarised Zone (DMZ)**

  The Processor has also implemented a firewall configuration respectively a demilitarised zone (DMZ) **(PCI-DSS requirement No. 1)** as well as a web-application firewall **(PCI-DSS requirement No. 6).** Details are being outlined in section „ General Data Processing System Access Control“.

- **Periodical Vulnerability Scans And Penetration Tests As Well As Use of Intrusion Detection and Intrusion Prevention Systems (IDS/IPS)**

  The Processor is periodically performing vulnerability scans as well as penetration tests from both inside and outside the network and corrects the possibly found exploitable vulnerabilities. Moreover, the Processor uses intrusion-detection and/or intrusion-prevention techniques which are giving an alert in case of suspected compromises (Intrusion Detection and Intrusion Prevention Systems, IDS/IPS). The aforementioned measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 11).**

- **Deployment Of Change-Detection Mechanisms For Unauthorised Modifications Of Critical System Files, Configuration Files, Or Content Files.**

In compliance with the requirements of the Data Security Standard of the Payment Card Industry, the Processor is deploying change-detection mechanisms which are giving an alert in case of unauthorised modifications (including changes, additions, and deletions) of critical system files, configuration files, or content files. Moreover, the Processor has implemented a process in order to respond to any such alerts **(PCI-DSS requirement No. 11).**

- **Development And Use Of Secure Systems And Applications**

  In compliance with the requirements of the Data Security Standard of the Payment Card Industry, the Processor is developing respectively using secure systems and is maintaining them accordingly. The PCI-DSS stipulates i.a. that security vulnerabilities are to be identified and all system components and software are to be protected from known vulnerabilities by installing applicable security patches in order to fix vulnerabilities. For in-house developed applications (such as, in particular, the Computop Paygate), in addition, criteria for secure development are being specified. Thus, after development, the custom code is to be reviewed in order to identify any potential coding vulnerabilities (four-eyes principle), if necessary, appropriate corrections are to be implemented. The final approval is being given by the management. For all changes to system components, change control processes and procedures are to be followed. Development environments respectively test environments are to be separated from the production environment. Moreover, common coding vulnerabilities in software-development processes are being addressed (e.g. injection flaws, buffer overflows, insecure cryptographic storage, insecure communications, improper error handling, cross-site scripting (XSS), improper access control or cross-site request forgery (CSRF)). According to the requirements of the PCI-DSS, developers are at least annually to be trained in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities, and the development of applications is to be based on secure coding guidelines. The aforementioned measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 6).**

  Furthermore, in compliance with the requirements of the Data Security Standard of the Payment Card Industry, before installing a system on the network, the Processor changes all default passwords and removes unnecessary default accounts. Moreover, he is developing configuration standards for all system components which adress all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Furthermore, as required for the function of the system, only necessary services, protocols and daemons are being enabled, where appropriate additional security features are being implemented and unnecessary functionalities (such as scripts, drivers, features, subsystems, file systems and unnecessary webservers) are being removed. The aforementioned measures are periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 2).**

- **Uninterruptible Power Supply (UPS)**

  The Processor is using systems for uninterruptible power supply (UPS systems) to provide a sufficient power supply for his systems.

- **Air Condition**

  All servers in use are being located in a climate-controlled environment.

- **Fire Protection**

  In all areas where data processing takes place, adequate fire protection measures have been taken for the respective specific area.

- **Incident Response Plan (Incident Response Management, Emergency Plan)**

  In compliance with the requirements of the Data Security Standard of the Payment Card Industry, the Processor has implemented an incident response plan which is being reviewed on a regular basis. The purpose of this incident response plan is to be prepared to immediately respond to security breaches in the system. According to the PCI-DSS, requirements for the content of an incident response plan are, in particular: The definition of roles, responsibilities and communication and contact strategies in the event of a compromise, including notification of the payment brands, the definition of specific incident response procedures, the definition of business recovery and continuity procedures, the definition of data backup processes, the analysis of legal requirements for reporting compromises, the coverage of all critical system components and a reference to or the inclusion of incident response procedures from the payment brands. Specific personnel is available on a 24/7 basis in order to respond to alerts. Staff with security breach response responsibilities is receiving appropriate training. Alerts from security monitoring systems are being taken into consideration. The aforementioned measure is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 12).**

5. Process For Regularly Testing, Assessing And Evaluating The Technical And Organisational Measures

- Article 32 Section 1 lit. d) GDPR -
Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.1 Job Control

✓CERTIFIED
according to PCI-DSS,
PCI-DSS in general

Measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the Controller.

- **PCI Certification**

  Job control in general takes place in the course of the annual certification according to the Data Security Standard of the Payment Card Industry **(PCI-DSS in general)** and the preparations for this. Within this certification, the Processor undergoes, in particular, strict external assessments of the technical and organisational measures.

- **Data Protection Officer**

  Moreover, the Processor has appointed a data protection officer who works towards ensuring compliance with the applicable data protection provisions.

- **Commitment To Data Secrecy And Confidentiality**

  Furthermore, the Processor is only using persons for the Processing on behalf of the Controller who have been committed in writing to the data secrecy and, according to the provisions of the GDPR, to confidentiality.

- **Formalised Placement Of Orders**

  The placement of orders by Controllers towards the Processor usually takes place in a formalised way via the oder forms and contractual documents provided by the Processor. This process for a formalised placement of orders serves the quality assurance regarding the performance of services by the Processor as contractually agreed.

5.2 Other Measures

✓CERTIFIED
according to PCI-DSS,
requirement No. 12
PCI-DSS in general,
PCI-P2PE and PCI-PIN

- **Process For Regularly Testing, Assessing And Evaluating The Effectiveness Of The Technical And Organisational Measures**

  A regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures takes place in the course of the preparations for the annually recurring assessments for the certifications after **PCI-DSS, PCI-P2PE and PCI-PIN.**

- **Internal Set Of Rules For IT Security**

  Computop has established an internal set of rules for data protection and IT security. In this context, also the requirements of the PCI-DSS regarding an information security policy are being implemented.

  This measure is periodically in detail being externally audited and certified after the Data Security Standard of the Payment Card Industry **(PCI-DSS requirement No. 12).**