GENERAL TERMS AND CONDITIONS

1. GENERAL PROVISIONS

1.1 This General terms and conditions govern your use of the Payment Gateway and together with the Standard Operating Procedure and the Processing Agreement executed between DominiPay (hereinafter – "Company") and the Client (hereinafter "Client" and "Company" jointly referred to as "Parties") constitute an entire agreement between Parties (hereinafter – "Agreement").

2. TERMS AND DEFINITIONS

2.1 If in accordance with the applied rules of the payment systems any term is supposed to have another meaning which is different from the one stated herein, such a term shall be interpreted in accordance with the rules of the payment system.

2.2 Terms used herein shall have the meaning specified in this clause, provided that they are capitalized:

2.2.1 "Acquirer" means a financial institute that performs full scope of financial transactions related to settlements and Card payments.

2.2.2 "Billing Error" shall mean a bona fide clerical, administrative or computational error, including an error in applying the rates expressly set out in the applicable fee schedule or pricing terms agreed between the Parties or an omission or duplication of chargeable Transactions and/or logged hours recorded in the applicable task management or ticketing system for billing purposes, but excluding any retroactive change to agreed rates, introduction of new charges, or any re-pricing of Services.

2.2.3 "Card" means the tool for cashless transfers, designed for the Cardholder to make transactions using money on the bank account opened by the Issuing Bank to the Cardholder's name under the agreement between such Cardholder and Issuing Bank.

2.2.4 "Cardholder" means an individual or an authorized representative of a legal entity, in whose name the Card is issued.

2.2.5 "Deposit to card transfer transaction (D2C)" shall mean any Transaction issued to Payment Gateway from Internet website or Mobile Internet website aimed at transfer of monetary funds from the bank account of the Client to the Card in favour of the Cardholder.

2.2.6 "E-Commerce payment transaction" shall mean any payment Transaction issued to Payment Gateway from Internet website or Mobile Internet website.

2.2.7 "Governmental Body" shall mean any government or governmental or regulatory body thereof, or political subdivision thereof, or any agency,

DRAFT - LEGAL REVIEW REQUIRED

instrumentality or authority thereof, or any court or arbitrator (public or private).

2.2.8 "Issuing Bank" means a bank, which issues and maintains the Card.

2.2.9 "Man Hour" means a unit for measuring working time equal to one hour of actual work of one person.

2.2.10 "Mobile payment transaction" shall mean any payment Transaction issued to Payment Gateway from Mobile terminal.

2.2.11 "Mobile Terminal" means an aggregate of a mobile device and a mobile POS-terminal connected to it, designed to read the Card data and used in order to process payment transactions and/or for information exchange with the Payment Gateway via the Payment Gateway.

2.2.12 "MOTO payment transaction" shall mean any payment transaction issued to Payment Gateway from a virtual terminal or e-terminal.

2.2.13 "Payment Gateway" means the hardware and software complex deployed at the Payment System, which allows to automate the process of acceptance and making of payments.

2.2.14 "Payment System" means the international payment system "Visa International", the international payment system "MasterCard Worldwide, and other operators on transfer of digital money.

2.2.15 "PCI DSS" (Payment Card Industry Data Security Standard) means the rules for secure storage, processing and transfer of data accepted in the payment cards industry and supported with the participation of Payment Systems.

2.2.16 "Personal Data Processing Agreement" shall refer to Appendix #1 attached to these General Terms and Conditions which constitutes an integral part of thereof.

2.2.17 "Processing Service" mean data processing and information exchange between Client, Acquirer and Cardholders via the Payment Gateway for purpose of making agreed Transactions.

2.2.18 "Processing Service" shall mean providing a safe software and technical infrastructure complying with the PCI DSS, for the purpose of secure exchange of data between settlements and data storage participants.

2.2.19 "Sanctions" shall mean any sanction administered or enforced by the United States Government (including without limitation, OFAC), the United Nations Security Council, the European Union, Her Majesty's Treasury ("HMT") or other relevant sanctions authority.

2.2.20 "Specification" shall mean a description of Payment Gateway, published at the Company website[1].

[1] https://dominipay.com

DRAFT - LEGAL REVIEW REQUIRED

2.2.21 "Standard operating procedure" means the procedure of communication between the Client and the Company is published at the Company website[2].

2.2.22 "The cardholder data environment (CDE)" mean comprised of people, processes and technologies that store, process, or transmit Cardholder data or sensitive authentication data.

2.2.23 "Transaction" means a payment transaction of settlement for products, works, and (or) services purchased (being purchased), executed with the use of the Card; or a financial transaction of transfer of funds with using Matercard Moneysend and Visa direct technologies.

2.2.24 DominiPay Analytics Analytical Platform") means the payment business management system and analytical platform of the Payment Gateway. Account in such system is provided to the Client after the execution of this Agreement.

2.2.25 Terms "Support System", "Account", "Error" used herein, shall have the meaning provided by the Standard Operating Procedure.

3. AVAILABILITY OF PAYMENT GATEWAY

3.1 The Company shall ensure accessibility of servers and databases of the Payment Gateway of no less than 99.0% of time per month (no more than 7.299 hours of downtime per month). Payment Gateway is deemed accessible if the servers it functions on work without Critical Errors as described in Standard operating procedure.

3.2 Payment Gateway is provided on the terms of Internet access to the servers, where the software and the database management systems are hosted via interfaces provided in the Payment Gateway.

3.3 To ensure the adequate level of quality and security Parties agreed to introduce the schedule of preventive maintenance works, during which time the Payment Gateway will be inaccessible. Procedure for preventive maintenance works is set forth in the Standard operating procedure. During the preventive maintenance works the Payment Gateway is deemed accessible despite the interruption.

3.4 Measuring the availability of the servers' connection with the Internet is carried out by an external monitoring service in accordance with Standard operating procedure.

3.5 Company shall take reasonable measures to ensure the proper and continuous operation of the Payment Gateway and provision of the Processing Service all as indicated under Standard Operating Procedure.

4. NEW INVENTIONS

4.1 OWNERSHIP OF NEW INVENTIONS

4.1.1 The Client shall acquire no rights to new enhancements, translations, re-writings, revisions, updates, modifications, or improvements made by Company/Client in connection with the Payment Gateway (hereinafter — "the New Inventions") which shall be considered as an integral part of the Payment

[2] https://dominipay.com

DRAFT - LEGAL REVIEW REQUIRED

Gateway, including but not limited to Acquirer integration software, from the moment of their creation unless parties agree to treat it differently and sign their intentions in the separate Agreement or Addendum to this contract.

4.2 IMPLEMENTATION

4.2.1 Company shall be entitled to implement, at any time, any New Invention at its own discretion without Client's consent, providing it does not influence the way the Client uses the system.

5. REPRESENTATIONS AND WARRANTIES OF COMPANY

5.1 Company hereby covenants, represents, and warrants to Client that:

(i) Company is a company validly existing and in good standing under applicable law Company has full corporate power and authority to own, lease and operate its property and to carry on its business as conducted and is duly qualified to transact business.

(ii) Company has full corporate power and authority to enter into and deliver the Agreement and all other agreements specified in or contemplated by the Agreement to be entered into and to perform its obligations hereunder and there under. The execution and delivery by Company of the Agreement and all other agreements specified in or contemplated by the Agreement to be entered into and the performance by Company of its obligations hereunder and there under have been duly authorized by all requisite action on its part.

(iii) The Agreement has been duly executed and delivered by Company and constitutes the legal, valid and binding obligation of Company enforceable against it in accordance with its terms. Company warranties to the Client that it has the rights to use and provide services based on the Payment Gateway.

(iv) Neither the execution and delivery by Company of the Agreement or any of the instruments or agreements herein referred to nor the consummation by it of any of the transactions contemplated hereby or thereby nor the performance by Company of the Agreement or any of the instruments or agreements herein referred to in accordance with their respective terms requires the consent, approval, order or authorization of, or registration with, or the giving of notice to any Governmental Body or any third party.

(v) Neither the execution and delivery by Company of the Agreement or any of the instruments or agreements herein referred to nor the consummation by it of any of the transactions contemplated hereby or thereby nor compliance by Company with any of their respective terms and provisions will contravene any applicable law or regulation or any judgment, decree or order applicable to or binding upon Company or will contravene or result in any breach of, or constitute any default under, its organizational documents or any agreement or instrument to which it is a party or by which it or any of its properties may be bound, or result in the creation of any Lien upon property of Company.

(vi) Company provides the Client with guarantees of security of the Payment Gateway in accordance with the current version of the PCI DSS. The Company acknowledges that it is responsible for the security of Cardholder data that is being stored, processed, or transmitted within the Cardholder Data Environment (CDE) owned and managed by the Company.

DRAFT - LEGAL REVIEW REQUIRED

6. REPRESENTATIONS AND WARRANTIES OF CLIENT

6.1 Client hereby covenants, represents, and warrants to Company that:

(i) Client has full corporate power and authority to own, lease and operate its property and to carry on its business as conducted and is duly qualified to transact business, and is in good standing, in all jurisdictions wherein the nature of its business or its ownership, lease or operation of property requires Client to be qualified as a foreign corporation or where the failure so to qualify might impair its right to enforce its contracts or expose it or its business, properties or assets to material liabilities.

(ii) Client has all the necessary licenses and permits for its business activities and will conduct its business in compliance with any and all laws and regulations applicable to the Client.

(iii) Client has full corporate power and authority to enter into and deliver the Agreement, General Terms and all other agreements specified in or contemplated by the Agreement to be entered into and to perform its obligations hereunder and there under. The execution and delivery by Client of the Agreement and all other agreements specified in or contemplated by the Agreement to be entered into and the performance by Client of its obligations hereunder and there under have been duly authorized by all requisite action on its part.

(iv) The Processing Agreement, the SOP, and the General Terms and all other agreements specified in or contemplated by the Agreement has been duly executed and delivered by Client and constitutes the legal, valid and binding obligation of Client enforceable against it in accordance with its terms.

(v) Neither the execution and delivery by Client of the Agreement or any of the instruments or agreements herein referred to nor the consummation by it of any of the transactions contemplated hereby or thereby nor the performance by Client of the Agreement or any of the instruments or agreements herein referred to in accordance with their respective terms requires the consent, approval, order or authorization of, or registration with, or the giving of notice to any Governmental Body or any third party.

(vi) Neither the execution and delivery by Client of the Agreement or any of the instruments or agreements herein referred to nor the consummation by it of any of the transactions contemplated hereby or thereby nor compliance by Client with any of their respective terms and provisions will contravene any existing law, rule or regulation or any judgment, decree or order applicable to or binding upon Client or will contravene or result in any breach of, or constitute any default under, its certificate of incorporation or by-laws or any agreement or instrument to which it is a party or by which it or any of its properties may be bound, or result in the creation of any Lien upon property of Client.

(vii) The Client warrants and declares that the Client will not, and will not allow its Affiliates or any third party to: (I) copy, sell, license, distribute, transfer, modify, adapt, translate, prepare derivative works from, decompile, reverse engineer, disassemble the Payment Gateway and any part or component thereof, or otherwise perform illegal acts in relation to the Payment Gateway; (II) use the Payment Gateway to access, copy, transfer, transcode or retransmit content in violation of any law or third party rights; or (III) remove, obscure, or alter copyright notices, trademarks, or other proprietary rights affixed to or contained within the Payment Gateway if applicable.

(viii) The Client acknowledges that the Company is sole a technology provider and is not and will at no event be deemed to be a party to any Transaction between the Client and

DRAFT - LEGAL REVIEW REQUIRED

its customers or brands. The Client will be sole and exclusively liable to its customers and brands and will be solely responsible to any relationships between the Client and its customers.

(ix) Neither the Client nor any of its subsidiaries nor, to the knowledge of the Client, any director, officer, agent, employee or affiliate of the Client or any of its subsidiaries (i) is, or is controlled or 50% or more owned in the aggregate by or is acting on behalf of, one or more individuals or entities that are currently the subject of any Sanctions administered or enforced by the United States, the United Nations Security Council, the European Union, a member state of the European Union (including sanctions administered or enforced by Her Majesty's Treasury of the United Kingdom) or other relevant sanctions authority (collectively, "Sanctions" and such persons, "Sanctioned Persons" and each such person, a "Sanctioned Person"), (ii) is located, organized or resident in a country or territory that is, or whose government is, the subject of Sanctions that broadly prohibit dealings with that country or territory (collectively, "Sanctioned Countries" and each, a "Sanctioned Country") or (iii) will, directly or indirectly, use the proceeds of Processing Service or otherwise make available such proceeds to any subsidiary, joint venture partner or other individual or entity in any manner that would result in a violation of any Sanctions by, or could result in the imposition of Sanctions against, any individual or entity. Neither the Client nor any of its subsidiaries has engaged in any dealings or transactions with or for the benefit of a Sanctioned Person, or with or in a Sanctioned Country, in the preceding 5 years, nor does the Client or any of its subsidiaries have any plans to engage in dealings or transactions with or for the benefit of a Sanctioned Person, or with or in a Sanctioned Country.

7. LIABILITY OF THE COMPANY

7.1 CLIENT ACKNOWLEDGES THAT THE PAYMENT GATEWAY, THE PROCESSING SERVICES AND/OR DOMINIPAY API HEREUNDER ARE PROVIDED "AS IS", AND COMPANY DOES NOT WARRANT THAT THE USE OF THE PAYMENT GATEWAY, THE PROCESSING SERVICES, AND/OR DOMINIPAY API FURNISHED IN CONNECTION WITH THIS AGREEMENT WILL BE UNINTERRUPTED OR ERROR-FREE. EXCEPT AS PROVIDED HEREIN THIS AGREEMENT, COMPANY PROVIDES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE PAYMENT GATEWAY OR THE PROCESSING SERVICE AND ITS FITNESS OR COMPATIBILITY WITH ANY PURPOSE.

7.2 Notwithstanding the aforesaid, the parties acknowledged that the use of the Payment Gateway is subject to factors which are not within Company's control. The Company shall not be liable to any failure in the provision of the Processing Service which is caused exclusively by factors which are not in Company's control.

7.3 The indemnification hereunder shall apply to all liabilities, damages, losses, expenses, claims, demands, suits proceedings, fines, judgments or execution proceedings (including without limitation, any reasonable legal fees, costs and related expenses) incurred or suffered by any indemnified party as a result of indemnified event as detailed above and any claims or proceedings brought by any third party arising out of or in connection with any breach of the indemnifying party's obligations under the Agreement, gross negligence or wilful misconduct on the part of the indemnifying party or anyone acting on its behalf.

DRAFT - LEGAL REVIEW REQUIRED

7.4 Notwithstanding anything in the Agreement, Company's total aggregate liability for all claims related to the Agreement, whether based on an action or claim in contract, tort (including negligence), breach of statutory duty or otherwise arising out of, or in relation to the Agreement, will be to 100% of the monthly average fees actually paid to the Company pursuant to the Agreement in the three (3) calendar month period prior to the cause of action giving rise to the first claim made under this Agreement.

7.5 NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR WILLFUL MISCONDUCT OR GROSS NEGLIGENCE, THE COMPANY SHALL BEAR NO LIABILITY TO THE CLIENT WITH RESPECT TO ANY AND ALL INDIRECT, CONSEQUENTIAL, INCIDENTAL AND PUNITIVE DAMAGES CAUSED TO THE CLIENT UNDER THIS AGREEMENT, INCLUDING BUT NOT LIMITED, LOSS OF DATA OR LOSS OF PROFITS, REGARDLESS IF COMPANY WAS ADVISED OF THE POSSIBLITY OF SUCH DAMAGES.

8. LIABILITY OF THE CLIENT

8.1 In the event of failure by the Client to pay any invoice on its due date, the Company will be entitled to suspend or terminate the license and services rendered to the Client under this Agreement with immediate effect upon notice to the Client, and in addition to any other remedy to which the Company is entitled under this Agreement or any applicable law.

8.2 Client shall defend, indemnify, and hold Company and its respective officers, directors, agents, employees harmless from claim, demand, fine, or other liability incurred by any such party due to or arising out of any breach of the Agreement by the Client or any party on Client's behalf.

9. CONSIDERATION, TAXES AND SETTELMENT CURRENCY

9.1 **Collection**. The Client is solely responsible for collection of payment from the Acquirer, and that the fees due to the Company are due to the Company without delay whether the Client collected payments from the Acquirer or not.

9.2 **Taxes**. The Client shall pay or reimburse to Company any applicable taxes and charges levied by any government authority on the services received by Client, including (not limited) value added tax, services tax.

9.3 **Settlement currency**. All sums of money due in consideration to the rendered services, will be calculated in invoices in euro currency. If some Transactions will be denominated in currencies other than euro, Company should apply exchange rate which is established by the European Central Bank (ECB) on date of each Transaction.

9.4 **Invoicing**. Company shall issue the Client an invoice for the fees due for the Processing Service once per month before the 7th day of the calendar month following the month in which the Processing Services have been rendered. Client will pay the invoice within ten (10) calendar days from receiving the invoice via e-mail.

9.5 **Invoice dispute procedure**. The Client has the right to submit a reasoned objection to the invoice within 10 (ten) calendar days from the date of issuance, providing an export of transactions processed through the provided channel or other relevant documentation for the applicable period, demonstrating an alternative remuneration amount due to the Company. If the Company does not provide a justified response

DRAFT - LEGAL REVIEW REQUIRED

disputing the Client's objection within 20 (twenty) business days, the invoice shall be considered contested by the Client and subject to reissuance by the Company.

9.6 Consequences of payment delay.

9.6.1 If the invoice remains unpaid for more than 20 (twenty) business days from the date of issuance and is not considered contested as per the procedure outlined above, the Company shall have the right to suspend all Processing Services provided under this Agreement. This suspension shall apply both to the Client and to all of the Client's customers utilizing the payment channel under this Agreement. The suspension shall remain in effect until full settlement of the outstanding debt. The Company shall provide the Client with a prior notice of at least 5 (five) business days before the suspension takes effect.

9.6.2 If the invoice remains unpaid for more than 30 (thirty) business days from the date of issuance and is not considered contested as per the procedure outlined above, the Company shall have the right to stop rendering Processing Services unilaterally and without judicial procedure, as well as to disable access to the Payment Gateway, including the provided DominiPay API and related technical support. However, the Company undertakes to provide the Client with a written notice of such suspension at least 5 (five) business days in advance via e-mail to the address specified in this Agreement. Additionally, the Company reserves the right to notify the Client's customers utilizing the Payment Gateway under this Agreement about the suspension or potential termination of the Processing Service.

9.6.3 The Company shall resume rendering the Processing Service and restore access to Payment Gateway, including the provided DominiPay API within 5 (five) business days after all outstanding amounts are settled.

9.7 If either Party discovers a Billing Error in any invoice issued under this Agreement, the Parties shall cooperate in good faith to correct such Billing Error.

9.7.1 **Overbilling**: where the Client has overpaid due to a Billing Error, the Company shall, at the Client's election, (i) issue a credit note (or correcting invoice) for the overbilled amount and refund the overpaid amount within thirty (30) days after the issuance of such credit note (or correcting invoice), or (ii) issue a credit note (or correcting invoice) and apply such amount as a credit against the next invoice(s). Any VAT charged on the overbilled amount shall be adjusted accordingly (if applicable).

9.7.2 **Underbilling**: where the Client has underpaid due to a Billing Error, the Company may invoice the underbilled amount, and such amount may be included in the next monthly invoice and shall be payable in accordance with the payment terms of this Agreement. No interest, penalties or late charges shall accrue solely in respect of the period prior to the issuance of the correcting invoice.

9.7.3 **Look-back limit**: no correction (and no claim for any underbilled amount) may be made in respect of Services performed more than twenty-four (24) months prior to the date on which the non-affected Party receives written notice (including by e-mail) of the relevant Billing Error together with reasonable supporting details.

DRAFT - LEGAL REVIEW REQUIRED

9.7.4 Any dispute as to whether a Billing Error exists or the amount of any correction shall be addressed under the invoice objection procedure set out above, and the undisputed portion shall remain payable when due.

10.TERMS AND TERMINATION

10.1 Term of the Agreement is one year from the day of signing the Agreement by both Parties. The Agreement is deemed prolonged for one year under the same terms and conditions each time provided that neither Party to the Agreement notifies the other Party about its intention to terminate the Agreement by sending written notice three (3) months prior to expiration of the Agreement term.

10.2 The Agreement may be terminated only as follows:

10.2.1 by mutual agreement of Company and Client; or

10.2.2 by Company unilaterally without any reason provided that the Company notifies the Client one (1) months in advance about Agreement termination; or

10.2.3 by Company in the event: (a) Client files a petition in bankruptcy; (b) Client is adjudicated as bankrupt or insolvent; (c) a petition in bankruptcy is filed against Client and such petition remains undismissed, unstayed or unbonded for a period of more than 90 days; (d) Client makes a general assignment for the benefit of its creditors or an arrangement pursuant to any bankruptcy law; (e) Client applies for or consents to the appointment of a receiver, trustee, custodian, sequestrate, liquidator or similar official for itself or any of its assets or properties; (f) Client fails or is unable, or admits in writing to its inability, to pay its debts generally as they become due; (g) Client conceals, removes or transfers any of its assets or properties in violation or evasion of any bankruptcy, fraudulent conveyance or similar applicable law; (h) Client discontinues its business; or (i) the Client breached the Agreement and fails to remedy such breach within seven (7) days following receipt of notice from the Company; or (j) Client takes any action for the purpose of effecting any of the foregoing; or by operation of law.

Notwithstanding the abovementioned, the Company will be entitled to terminate this Agreement with immediate effect by providing the Client with notice in the event the Company is prohibited from providing the License or the Processing Service by any regulative, legal or governmental authorities.

10.2.4 By the Client unilaterally and without any reason provided that the Company is provided with three (3) months written advance notice; or

10.2.5 By the Client in the event (a) Company files a petition in bankruptcy; (b) Company is adjudicated as bankrupt or insolvent; (c) a petition in bankruptcy is filed against Company and such petition remains undismissed, unstayed or unbonded for a period of more than 90 days; (d) Company makes a general assignment for the benefit of its creditors or an arrangement pursuant to any bankruptcy law; (e) Company applies for or consents to the appointment of a receiver, trustee, custodian, sequestrate, liquidator or similar official for itself or any of its assets or properties; (f) Company fails or is unable, or admits in writing to its inability, to provide the Services in accordance to the Agreement; (g) Company conceals, removes or transfers any of its assets or properties in

DRAFT - LEGAL REVIEW REQUIRED

violation or evasion of any bankruptcy, fraudulent conveyance or similar applicable law; (h) Company discontinues its business; or (i) Company takes any action for the purpose of effecting any of the foregoing; or by operation of law.

10.3 Any provisions of the Agreement, including the General Terms and all other agreements specified in or contemplated by the Agreement which by their nature should survive the termination of the Agreement, will survive the termination thereof.

11.CONFIDENTIAL INFORMATION

11.1 "**Confidential Information**" shall mean any information disclosed by either party (the "Disclosing Party") to the other party or anyone acting in its behalf (the "Receiving Party") or by its Affiliates, in any manner: directly or indirectly, in writing, orally, in digital form or in any other form or media, including, without limitation, data, technology, Payment Gateway and modifications or upgrades thereof, the Processing Service, know-how, designs, processes, documents, systems, specifications, plans, Personal Data, ESK issued by the Client, information concerning research and development work, prices, costs, proposed transaction terms and other commercial information and/or trade and business secrets including information which relates to current, planned or proposed products, marketing, sales and business plans or status, forecasts, projections and analyses, financial information, third party confidential information and customer information, including Clients, Acquirers, PSPs, Transactions and parties to Transactions, vulnerabilities found in the Payment Gateway infrastructure.

11.2 EXCEPTIONS TO CONFIDENTIAL INFORMATION

11.2.1 For the purposes of this Agreement, Confidential Information will not include any information that has been:

11.2.1.1 publicly known and made generally available in the public domain, through no action or inaction of the parties;

11.2.1.2 already in the possession of the Receiving Party at the time of disclosure by a Disclosing Party, as demonstrated by documentary evidence;

11.2.1.3 obtained by the Receiving Party from a third party without a breach of such third party's obligations of confidentiality, as demonstrated by documentary evidence; or;

11.2.1.4 independently developed by the Receiving Party without use of or reference to the Confidential Information, as demonstrated by documentary evidence.

11.3 RESTRICTIONS ON USE

11.3.1 Receiving Party agrees and undertakes that it will not use the Confidential Information except in accordance with the purpose of this Agreement nor will it disclose any Confidential Information to any third parties without the Disclosing Party's written consent.

11.3.2 Receiving Party may disclose the Confidential Information if required by law, so long as it gives the Disclosing Party prompt written notice of such requirement prior to such disclosure (unless such notice is prohibited by law) and assistance

DRAFT - LEGAL REVIEW REQUIRED

in obtaining an order protecting the Confidential Information from public disclosure. If such an order is not obtained, Receiving Party shall disclose only that portion of the Confidential Information which is legally required, and shall ensure confidential treatment of such information.

11.3.3 Except for backup of the Confidential Information, Receiving Party shall not make any copies of any Confidential Information without the prior written consent of the Disclosing Party.

11.4 STANDARD OF CARE

11.4.1 Receiving Party agrees that it shall hold all Confidential Information in strict confidence and shall safeguard the Confidential Information with the highest reasonable degree of care, while taking all reasonable precautions necessary to protect the secrecy and preserve the confidentiality of the Confidential Information.

11.4.2 Without limiting the foregoing, Receiving Party will take at least those measures that it takes to protect its own confidential information but take not less than reasonable measures and utilize not less than a reasonable standard of care.

11.5 PERMITTED DISCLOSURE

11.5.1 Receiving Party agrees not to disclose, even in part, any Confidential Information, except as provided herein. Receiving Party shall only make the Confidential Information, and even then, specifically the relevant parts thereof, available to its employees, consultants, affiliates, agents and subcontractors, excluding any entity (and any personnel of such entity) that is a competitor of the Disclosing Party, on a "need to know" basis in order to carry out the purpose of the Agreement (such recipients, collectively, the "Authorized Recipients").

11.5.2 Prior to any disclosure of the Disclosing Party's Confidential Information to the Authorized Recipients to the extent permitted hereunder, the Receiving Party will ensure that such Authorized Recipients are bound by a non-use and non-disclosure agreement that contains provisions in respect of disclosure and use of Confidential Information that are substantially similar to the applicable provisions of this clause. Furthermore, each party will reproduce the other party's proprietary rights and confidentiality notices on any approved copies of Confidential Information.

11.6 INJUNCTIVE RELIEF

11.6.1 The parties acknowledge that unauthorized disclosure or use of Confidential Information may give rise to irreparable injury, which may not be adequately compensated by damages. The Parties agree and acknowledge that money damages may not be a sufficient remedy for any breach or threatened breach of this Agreement by either party and that the other party shall be entitled to seek specific performance or injunctive relief (as appropriate) as a remedy for any breach or threatened breach thereof, in addition to any other remedies available at law or in equity.

11.7 RETURN OF MATERIALS

11.7.1 Upon the written request of the Disclosing Party, the Receiving Party shall promptly return to the Disclosing Party or destroy all copies of the Confidential

DRAFT - LEGAL REVIEW REQUIRED

Information. Receiving Party shall furnish the Disclosing Party, together with such returned materials or subsequent to any destruction thereof, a certificate duly executed by an officer of such party, confirming that the provisions of this section have been complied with. Return or destruction of the Confidential Information as required hereunder shall not affect the remaining obligations pursuant to this Agreement.

12.FORCE MAJEURE

12.1 If performance by any Party of any service or obligation under this Agreement is prevented, restricted, delayed or interfered with by reason of, inter alia, strikes, acts of God, fire, floods, lightning, earthquakes, severe weather, utility or communication failures, failures of any relevant bank or network, DDoS attacks, computer associated outages or delay in receiving electronic data, war, civil commotion, or any law, order or regulation, etc. having legal effect, then that Party shall be excused from its performance hereunder to the extent and duration of the prevention, restriction, delay or interference.

13.INFRINGEMENTS

13.1 Each Party shall promptly upon learning of same notify the other Party of the facts and circumstances surrounding any alleged infringement of the rights or misappropriation of the rights or any right of either party known to the other Party hereto.

14.MISCELLANEOUS

14.1 ASSIGNMENT. Client shall not assign or transfer the Agreement or any part thereof to any other entity without the prior written consent of the Company. The Company will be entitled to assign this Agreement by notifying the Client. Upon assignment to an Affiliate, the references in the Agreement to Company or Client, as applicable, shall also apply to any such assignee unless the context otherwise requires.

14.2 NO PARTNERSHIP OR JOINT VENTURE. Nothing herein contained shall be construed to place the parties in relationship of partners or joint ventures, and neither party shall have the power to obligate or bind the other party in any manner whatsoever.

14.3 SEVERABILITY. If any provision or provisions of the Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.

14.4 COMMUNICATION BETWEEN PARTIES. Communication between Parties shall be performed in accordance with the order stated in Standard operating procedure.

14.5 DISPUTE RESOLUTION. Any dispute, controversy or claim between the Parties hereto arising out of or relating to this Agreement or any alleged breach thereof which cannot be amicably settled between the parties shall be exclusively referred to arbitration in accordance with the applicable arbitration law

14.6 GOVERNING LAW & JURISDICTION. This agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-

DRAFT - LEGAL REVIEW REQUIRED

contractual disputes or claims) shall be governed exclusively by and construed in accordance with the applicable law

14.7 COSTS AND EXPENSES. Company and Client shall each bear its own costs and expenses incurred in connection with the negotiation and execution of the Agreement and each other agreement, document and instrument contemplated by the Agreement and the consummation of the transactions contemplated hereby and thereby.

14.8 HEADINGS. The headings used in the Agreement are for convenience only and do not define, limit or construe the contents thereof.

14.9 CONSTRUCTION. Whenever used in the Agreement, the singular shall be construed to include the plural and vice versa, where applicable, and the use of the masculine, feminine or neuter gender shall include the other genders.

14.10 COUNTERPARTS. This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

14.11 THIRD-PARTY CONTRACTS. The Company may enter any agreements and sign appropriate contracts required to deliver its services, e.g. with banks, third-party PSPs or any other organizations, including the ones that have relations with the Client.

14.12 THIRD PARTY RIGHTS. A Person who is not a party to this agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this agreement. The rights of the parties to terminate, rescind or agree any variation, waiver or settlement under this agreement are not subject to the consent of any other person.

14.13 RESPONSIBILITY. Client shall independently render services to its contract partners, Company bears no responsibility for the activity performed by Client.

DRAFT - LEGAL REVIEW REQUIRED

PERSONAL DATA PROCESSING AGREEMENT

1. OVERVIEW

1.1 The Parties comply with global data protection regulations and requires all own suppliers to verify their compliance. Whereas the Client has entered into a Service Agreement to provide services involving the processing of Client personal data. The Company must certify their compliance with GDPR and other data protection regulations.

1.2 Where this Personal Data Processing Agreement ("PDPA") use the terms defined in Regulation (EU) 2016/679 ("GDPR") respectively, those terms shall have the same meaning as in that Regulation.

2. ROLES OF THE PARTIES

2.1 In the context of the Service Agreement, the Parties agree that Company acts as Processor acting on behalf of Client who act as Controllers.

2.2 Client appoints Company as Processor, or as Sub-Processor of Client's customers (in particular Cardholders), for the Personal Data Processing for the purpose of providing the Processing Service specified in Service Agreement. In that context, Client, as Controller, or Processor acting on behalf of its customers, has the sole and exclusive authority to determine the purposes and means of the Personal Data Processing that are disclosed to and collected by Company. Company will Process Personal Data only on behalf and for the benefit of Client, or of Client's customers, and only to carry out its obligations under this Service Agreement as implemented and to the extent required for execution of the Service Agreement.

3. PROCESSING

3.1 The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Annex I.

4. OBLIGATIONS OF THE PROCESSOR

4.1 The Processor shall process personal data related to cardholder information, including the primary account number (PAN), expiration date, and cardholder name, in accordance with PCI DSS requirements. Such data shall be stored in encrypted form using appropriate technical and organizational measures to ensure data security, as required under Article 32 of the GDPR.

DRAFT - LEGAL REVIEW REQUIRED

4.2 Other data required for operational access shall not be encrypted. However, access to such data shall only be provided to authorized users following a successful authorization process. All access instances shall be logged, including the time and identity of the individual accessing the data.

4.3 The Processor guarantees compliance with all GDPR requirements, including restricting access to personal data and ensuring transparency of all processing activities involving such data.

4.4 The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by European Union or Member State law to which the Processor is subject. In such cases, the Processor shall inform the Controller of that legal requirement before processing, unless prohibited by law on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data, provided such instructions are documented and do not contradict the data processing provisions set forth above, including those regarding encryption and access control measures.

4.5 The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe GDPR, or the applicable European Union or Member State data protection provisions.

4.6 **Purpose limitation**. The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless it receives further instructions from the Controller.

4.7 **Duration of the processing of personal data**. Processing by the Processor shall only take place for the duration specified in Annex I.

4.8 **Security of processing**. The Processor shall at least implement the technical and organisational measures specified in Annex II to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.9 **Sensitive data**. The Processor shall not process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data") by default, as such data are not required for the purposes of payment processing.

The Controller further undertakes not to transmit such data to the DominiPay payment gateway via API or to submit them through UI interfaces under any circumstances. The Controller shall implement appropriate technical and organizational measures to prevent the transmission or inclusion of such sensitive data.

DRAFT - LEGAL REVIEW REQUIRED

4.10 **Response to Controller Inquiries**. The Processor shall respond promptly and adequately to inquiries from the Controller about the processing of data in accordance with the PDPA, with a maximum response time of three (3) business days. The Controller shall ensure that such inquiries are justified, reasonable, and not excessive in nature, taking into account the scope and purpose of the processing activities. Such inquiries must be submitted exclusively through agreed communication channels, which include either the creation of tickets in the task management system Redmine (redmine.clubber.me), access to which is provided by the Processor, or by sending an email which mentioned in cl. 9.1.

4.11 **Compliance with GDPR**. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in the PDPA and stem directly from GDPR. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by the PDPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the processor.

The conduct of audits, including their frequency and scope, shall be governed by the provisions set forth in Annex III. The Processor shall facilitate such audits in accordance with the agreed technical and organizational measures detailed in Annex III, ensuring that the process is aligned with the principles of necessity and proportionality.

The Parties shall make the information referred to in this PDPA, including the results of any audits, available to the competent supervisory authority/ies on request.

4.12 **Use of sub-processors**. The Processor shall not subcontract any of its processing operations performed on behalf of the Controller in accordance with this PDPA to a sub-processor, without the Controller's prior specific written authorisation. The Processor shall submit the request for specific authorisation at least three (3) business days prior to the engagement of the sub-processor in question, together with the information necessary to enable the Controller to decide on the authorisation. The list of sub-processors authorised by the Controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

4.13 **Cross border transfers**. Any transfer of data to a third country or an international organisation by the Processor shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under Union or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of GDPR.

The Controller agrees that where the Processor engages a sub-processor in accordance with cl. 4.12 for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of GDPR, the Processor and the sub-processor can ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of GDPR, provided the conditions for the use of those standard contractual clauses are met.

DRAFT - LEGAL REVIEW REQUIRED

5. ASSISTANCE TO THE CONTROLLER

5.1 The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the Controller.

5.2 The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. The Processor shall comply with the Controller's instructions.

5.3 In addition to the Processor's obligation to assist the Controller pursuant to cl. 5.2, the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processor:

a) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

b) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

c) the obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

d) the obligations in Article 32 of GDPR.

The Parties shall set out in Annex IV the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this PDPA as well as the scope and the extent of the assistance required.

6. PERSONAL DATA BREACH

6.1 In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 GDPR, where applicable, taking into account the nature of processing and the information available to the Processor.

6.2 In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

6.2.1 in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

6.2.2 in obtaining the following information which, pursuant to Article 33(3) of GDPR, shall be stated in the Controller's notification, and must at least include:

a) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) the likely consequences of the personal data breach;

DRAFT - LEGAL REVIEW REQUIRED

c) the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay in complying, pursuant to Article 34 of GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

6.3 In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Annex V set out all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of GDPR.

7. TERMINATION

7.1 Without prejudice to any provisions of GDPR provisions, in the event that the Processor is in breach of its obligations under this PDPA, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with this PDPA or the Agreement is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with this PDPA, for whatever reason.

7.2 The Controller shall be entitled to terminate the Agreement insofar as it concerns processing of personal data in accordance with the PDPA if:

a. the processing of personal data by the Processor has been suspended by the Controller pursuant to cl. 7.1 and if compliance with the PDPA is not restored within a reasonable time and in any event within one month following suspension;

b. the Processor is in substantial or persistent breach of this Agreement or its obligations under GDPR;

c. the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this Agreement or to GDPR.

DRAFT - LEGAL REVIEW REQUIRED

7.3 The Processor shall be entitled to terminate this Agreement insofar as it concerns processing of personal data under the PDPA where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with cl. 4.5, the Controller insists on compliance with the instructions.

8. CONSEQUENCES OF TERMINATION

8.1 Termination of this Data Processing Agreement shall result in the immediate cessation of payment processing services provided by the Company. Such termination shall also be deemed by the Parties as an expression of intent to terminate the entirety of the agreement governing the provision of payment processing services and access to the DominiPay payment gateway.

8.2 Following the termination of this Agreement, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller or return it to the Controller and delete existing copies, unless the retention of such data is required by European Union or Member State law. Notwithstanding this, the Processor may retain data related to payment card information, including the card number (PAN), expiration date, and cardholder name, as well as data related to transactions performed using such cards, including the transaction amount, currency, and associated logs, to the extent necessary to comply with PCI DSS standards or other applicable legal requirements.

The Processor undertakes to complete the deletion of all other personal data within one (1) year from the date of termination of the Agreement. Until the data is deleted or returned, the Processor shall ensure compliance with the provisions of this Agreement, including maintaining the security and confidentiality of the retained data as prescribed by the PDPA.

9. THE COMPANY'S DPO

9.1 Client's staff and customers may contact Company's DPO via e-mail: privacy@dominipay.com

DRAFT - LEGAL REVIEW REQUIRED

LIST OF PROCESSING PERSONAL DATA

Category	Purposes of Processing	Processing Term
First name	Processing payments and fulfilling obligations under the Principal Agreement under with PCI DSS compliance	5 years
Last name	Processing payments and fulfilling obligations under the Principal Agreement under with PCI DSS compliance	5 years
Address	Processing payments and fulfilling obligations under the Principal Agreement	5 years
Country	Processing payments and fulfilling obligations under the Principal Agreement	5 years
Email	Processing payments and fulfilling obligations under the Principal Agreement	5 years
Date of birth	Processing payments and fulfilling obligations under the Principal Agreement	5 years
Mobile number	Processing payments and fulfilling obligations under the Principal Agreement	5 years
IP Address	Processing payments and fulfilling obligations under the Principal Agreement	5 years
Browser data (e.g., userAgent, language, platform, etc.)	Fraud prevention, user authentication, and compliance with applicable security standards	5 years

DRAFT - LEGAL REVIEW REQUIRED

TECHNICAL AND ORGANISATIONAL MEASURES

The Company confirms that Personal Data is being processed within the Company's Cardholder Data Environment (CDE) i.e. Trusted Network of the Company where applicable security controls are applied to Payment Data Processing containing Personal and Cardholder Data. These requirements are standardized and mandated by International Payment Systems (Card Schemes) within the Payment Card Industry Data Security Standard (PCI DSS).

The following Data Security Requirements are met by the Company and annually audited by a third-party organization called Qualified Security Assessor (QSA). Where requirements affect or related to Personal Data with some specifics it is correspondingly commented.

1. REQUIREMENT 1. *INSTALL AND MAINTAIN NETWORK SECURITY CONTROLS*

1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood

The company maintains a set of documented policies and operational procedures which related to establishing and maintaining network security controls.

Roles and responsibilities for performing activities are documented, assigned and understood.

1.2 Network security controls (NSC) are configured and maintained

The company establishes and maintain processes within which the following network security controls are implemented:

- Configuration standards for NSC rulesets are:
  - Defined.
  - Implemented.
  - Maintained.
- All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process
- An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks
- An accurate data-flow diagram(s) is maintained
- All services, protocols, and ports allowed are identified, approved, and have a defined business need
- Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated
- Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective
- Configuration files for NSCs are:

DRAFT - LEGAL REVIEW REQUIRED

- Secured from unauthorized access.
- Kept consistent with active network configurations.

1.3 Network access to and from the CDE is restricted.

- Inbound traffic to the CDE is restricted as follows:
  - To only traffic that is necessary.
  - All other traffic is specifically denied.
- Outbound traffic from the CDE is restricted as follows:
  - To only traffic that is necessary.
  - All other traffic is specifically denied.

1.4 Network connections between trusted and untrusted networks are controlled

- NSCs are implemented between trusted and untrusted networks.
- Inbound traffic from untrusted networks to trusted networks is restricted to:
  - Communications with system components that are authorized to provide publicly accessible services, protocols, and ports.
  - Stateful responses to communications initiated by system components in a trusted network.
  - All other traffic is denied.
- Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.
- System components that store cardholder data and personal data are not directly accessible from untrusted networks.
- The disclosure of internal IP addresses and routing information is limited to only authorized parties.

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows:

- Specific configuration settings are defined to prevent threats being introduced into the entity's network.
- Security controls are actively running.
- Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.

2. REQUIREMENT 2: APPLY SECURE CONFIGURATIONS TO ALL SYSTEM COMPONENTS

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood

DRAFT - LEGAL REVIEW REQUIRED

The company maintains a set of documented policies and operational procedures which related to establishing and maintaining securing configurations to all system components.

Roles and responsibilities for performing activities are documented, assigned and understood.

2.2 System components are configured and managed securely

- Configuration standards are developed, implemented, and maintained to:
    - Cover all system components.
    - Address all known security vulnerabilities.
    - Be consistent with industry-accepted system hardening standards or vendor hardening recommendations.
    - Be updated as new vulnerability issues are identified.
    - Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.
- Vendor default accounts are managed as follows:
    - If the vendor default account(s) will be used, the default password is changed.
    - If the vendor default account(s) will not be used, the account is removed or disabled.
- Primary functions requiring different security levels are managed as follows:
    - Only one primary function exists on a system component,

  OR

    - Primary functions with differing security levels that exist on the same system component are isolated from each other,

  OR

    - Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.
- Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
- If any insecure services, protocols, or daemons are present:
    - Business justification is documented.
    - Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.
- System security parameters are configured to prevent misuse
- All non-console administrative access is encrypted using strong cryptography.

2.3 Wireless environments are configured and managed securely.

The company does not own or maintain wireless environments connected to the CDE.

DRAFT - LEGAL REVIEW REQUIRED

3. REQUIREMENT 3: PROTECT STORED ACCOUNT DATA AND PERSONAL DATA

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

The company maintains a set of documented policies and operational procedures which related to protection of the stored account data.

Roles and responsibilities for performing activities are documented, assigned and understood.

3.2 Storage of account data and Personal Data is kept to a minimum.

- Account data and Personal Data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes.

3.3 Sensitive authentication data (SAD) is not stored after authorization.

- SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.
- The full contents of any track are not stored upon completion of the authorization process.
- The card verification code is not stored upon completion of the authorization process.
- Personal Identification Number (PIN) is not processed.
- SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.

3.4 Access to displays of full PAN, Personal Data and ability to copy PAN, Personal Data are restricted.

- PAN is masked when displayed. There is no way to get full PAN displayed through the user interface.
- Personal Data is masked by default. Access to the Personal Data is allowed through granting special privileges.
- When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.

3.5 Primary account number (PAN) is secured wherever it is stored.

- PAN is rendered unreadable anywhere it is stored.
- Hashes used to render PAN unreadable are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures.

3.6 Cryptographic keys used to protect stored account data are secured.

- Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse.

DRAFT - LEGAL REVIEW REQUIRED

- Accurate details of the cryptographic architecture are maintained and available.
- Secret and private keys are stored in a secure form that prevents unauthorized retrieval or access.
- Access to cleartext cryptographic key components is restricted to necessary personnel.
- Cryptographic keys are retained only where necessary.

3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

- Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.
- Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.
- Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.
- Cryptographic keys are not used beyond their defined cryptoperiod.
- Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.
- Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person.
- Cryptographic keys cannot be substituted by unauthorized personnel.
- Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.
- Customers are provided with appropriate key management guidance whenever they receive shared cryptographic keys.

DRAFT - LEGAL REVIEW REQUIRED

4. REQUIREMENT 4: PROTECT CARDHOLDER DATA WITH STRONG CRYPTOGRAPHY DURING TRANSMISSION OVER OPEN, PUBLIC NETWORKS

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.

The company maintains a set of documented policies and operational procedures which related to protection of the account data during transmission over open, public networks.

Roles and responsibilities for performing activities are documented, assigned and understood.

4.2 PAN and Personal Data are protected with strong cryptography during transmission.

- Strong cryptography and security protocols are implemented as follows to safeguard PAN and Personal Data during transmission over open, public networks:
    - Only trusted keys and certificates are accepted.
    - Certificates used to safeguard PAN and Personal Data during transmission over open, public networks are confirmed as valid and are not expired or revoked.
    - The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.
    - The encryption strength is appropriate for the encryption methodology in use.
- An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.
- PAN and Personal Data are secured with strong cryptography whenever it is sent via end-user messaging technologies.

5. REQUIREMENT 5: PROTECT ALL SYSTEMS AND NETWORKS FROM MALICIOUS SOFTWARE

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

The company maintains a set of documented policies and operational procedures which related to protection all systems and networks from malicious software.

Roles and responsibilities for performing activities are documented, assigned and understood.

5.2 Malicious software (malware) is prevented, or detected and addressed.

- An anti-malware solution(s) is deployed on all system components.

DRAFT - LEGAL REVIEW REQUIRED

- The deployed anti-malware solution(s):
    - Detects all known types of malware.
    - Removes, blocks, or contains all known types of malware.

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

- Anti-malware mechanisms can detect and address the latest malware threats.
- The anti-malware solution(s) performs periodic scans and active or real-time scans.
- Malware cannot be introduced to system components via external removable media.
- Historical records of anti-malware actions are immediately available and retained for at least 12 months.
- Anti-malware mechanisms cannot be modified by unauthorized personnel.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.

6. REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND SOFTWARE

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

The company maintains a set of documented policies and operational procedures which related to development and maintenance of secure systems and software.

Roles and responsibilities for performing activities are documented, assigned and understood.

6.2 Bespoke and custom software are developed securely.

- Bespoke and custom software are developed securely, as follows:
    - Based on industry standards and/or best practices for secure development.
    - In accordance with PCI DSS (for example, secure authentication and logging).
    - Incorporating consideration of information security issues during each stage of the software development lifecycle.
- Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:
    - On software security relevant to their job function and development languages.
    - Including secure software design and secure coding techniques.
    - Including, if security testing tools are used, how to use the tools for detecting

DRAFT - LEGAL REVIEW REQUIRED

vulnerabilities in software.

- Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:
    - Code reviews ensure code is developed according to secure coding guidelines.
    - Code reviews look for both existing and emerging software vulnerabilities.
    - Appropriate corrections are implemented prior to release.
- Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software.

6.3 Security vulnerabilities are identified and addressed.

- New system and software vulnerabilities that may impact the security of cardholder data and/or sensitive authentication data are monitored, cataloged, and risk assessed.
- All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:
    - Patches/updates for critical vulnerabilities are installed within one month of release.
    - All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment.

6.4 Public-facing web applications are protected against attacks.

- For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:
    - Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:
        - Installed in front of public-facing web applications to detect and prevent web-based attacks.
            - Actively running and up to date as applicable.
            - Generating audit logs.
            - Configured to either block web-based attacks or generate an alert that is immediately investigated.

6.5 Changes to all system components are managed securely.

- Changes to all system components in the production environment are made according to established procedures that include:

DRAFT - LEGAL REVIEW REQUIRED

- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested before being deployed into production.
- Procedures to address failures and return to a secure state.

- Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
- Pre-production environments are separated from production environments and the separation is enforced with access controls.
- Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
- Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.
- Test data and test accounts are removed from system components before the system goes into production.

7. REQUIREMENT 7: RESTRICT ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA BY BUSINESS NEED TO KNOW

7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

The company maintains a set of documented policies and operational procedures that restrict access to system components and cardholder data by business.

Roles and responsibilities for restricting access to system components and cardholder data are assigned and understood.

7.2 Access to system components and data is appropriately defined and assigned.

- An access control model is defined and includes granting access as follows:
  - Appropriate access depending on the entity's business and access needs.
  - Access to system components and data resources that is based on users' job classification and functions.
  - The least privileges required (for example, user, administrator) to perform a job function.

DRAFT - LEGAL REVIEW REQUIRED

- Access is assigned to users, including privileged users, based on:
    - Job classification and function.
    - Least privileges necessary to perform job responsibilities.
- Required privileges are approved by authorized personnel.
- All user access to query repositories of stored cardholder data is restricted as follows:
    - Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges.
    - Only the responsible administrator(s) can directly access or query repositories of stored CHD.

7.3 Access to system components and data is managed via an access control system(s).

- An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.
- The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.
- The access control system(s) is set to "deny all" by default.

8. REQUIREMENT 8: IDENTIFY USERS AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

The company maintains a set of documented policies and operational procedures that identify users and authenticate access to system components.

Roles and responsibilities for identifying users and authenticating access to system components are assigned and understood.

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

- All users are assigned a unique ID before access to system components or cardholder data is allowed.
- Group, shared, or generic IDs, or other shared authentication credentials are only used when necessary, on an exception basis, and are managed as follows:
    - ID use is prevented unless needed for an exceptional circumstance.
    - Use is limited to the time needed for the exceptional circumstance.
    - Business justification for use is documented.

DRAFT - LEGAL REVIEW REQUIRED

    - Use is explicitly approved by management.
    - Individual user identity is confirmed before access to an account is granted.
    - Every action taken is attributable to an individual user.
- Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:
    - Authorized with the appropriate approval.
    - Implemented with only the privileges specified on the documented approval.
- Access for terminated users is immediately revoked.
- Inactive user accounts are removed or disabled within 90 days of inactivity.
- Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:
    - Enabled only during the time period needed and disabled when not in use.
    - Use is monitored for unexpected activity.
- If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.

8.3 Strong authentication for users and administrators is established and managed.

- All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
    - Something you know, such as a password or passphrase.
    - Something you have, such as a token device or smart card.
    - Something you are, such as a biometric element.
- Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.
- User identity is verified before modifying any authentication factor.
- Invalid authentication attempts are limited by:
    - Locking out the user ID after not more than 10 attempts.
    - Setting the lockout duration to a minimum of 30 minutes or until the user’s identity is confirmed.
- If passwords/passphrases are used as authentication factors, they are set and reset for each user as follows:
    - Set to a unique value for first-time use and upon reset.

DRAFT - LEGAL REVIEW REQUIRED

    - Forced to be changed immediately after the first use.

- Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.

- Authentication policies and procedures are documented and communicated to all users including:

    - Guidance on selecting strong authentication factors.

    - Guidance for how users should protect their authentication factors.

    - Instructions not to reuse previously used passwords/passphrases.

    - Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

- Password/passphrases are changed at least once every 90 days.

8.4 Multi-factor authentication (hereinafter – "MFA") is implemented to secure access into the CDE.

- MFA is implemented for all non-console access into the CDE for personnel with administrative access.

- MFA is implemented for all non-console access into the CDE.

- MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE.

8.5 MFA systems are configured to prevent misuse. MFA systems are implemented as follows:

- The MFA system is not susceptible to replay attacks.

- MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.

- At least two different types of authentication factors are used.

- Success of all authentication factors is required before access is granted.

8.6 Use of application and system accounts and associated authentication factors is strictly managed. Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.

DRAFT - LEGAL REVIEW REQUIRED

9. REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

The company maintains a set of documented policies and operational procedures that restrict physical access to cardholder data.

Roles and responsibilities for restricting physical access to cardholder data are assigned and understood.

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

- Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.
- Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.
- Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.
- Access to consoles in sensitive areas is restricted via locking when not in use.

9.3 Physical access for personnel and visitors is authorized and managed.

- Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including:
    - Identifying personnel.
    - Managing changes to an individual's physical access requirements.
    - Revoking or terminating personnel identification.
    - Limiting access to the identification process or system to authorized personnel.
- Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including:
    - Identifying personnel.
    - Managing changes to an individual's physical access requirements.
    - Revoking or terminating personnel identification.
    - Limiting access to the identification process or system to authorized personnel.
- Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.

DRAFT - LEGAL REVIEW REQUIRED

- Visitor logs are used to maintain a physical record of visitor activity both within the facility and within sensitive areas, including:
    - The visitor's name and the organization represented.
    - The date and time of the visit.
    - The name of the personnel authorizing physical access.
    - Retaining the log for at least three months, unless otherwise restricted by law.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

- All media with cardholder data is classified in accordance with the sensitivity of the data.
- Media with cardholder data sent outside the facility is secured as follows:
    - Media sent outside the facility is logged.
    - Media is sent by secured courier or other delivery method that can be accurately tracked.
    - Offsite tracking logs include details about media location.
- Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).
- Inventory logs of all electronic media with cardholder data are maintained.
- Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following:
    - The electronic media is destroyed.
    - The cardholder data is rendered unrecoverable so that it cannot be reconstructed.

9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution. POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:

- Maintaining a list of POI devices.
- Periodically inspecting POI devices to look for tampering or unauthorized substitution.
- Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

DRAFT - LEGAL REVIEW REQUIRED

10. REQUIREMENT 10: LOG AND MONITOR ALL ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.

The company maintains a set of documented policies and operational procedures that define processes and mechanisms for logging and monitoring all access to system components and cardholder data.

Roles and responsibilities for logging and monitoring all access to system components and cardholder data are assigned and understood.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. Audit logs are enabled and active for all system components and cardholder data.

10.3 Audit logs are protected from destruction and unauthorized modifications.

- Read access to audit logs files is limited to those with a job-related need.
- Audit log files are protected to prevent modifications by individuals.
- Audit log files, including those for external- facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.
- File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts. Audit log files, including those for external- facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

- The following audit logs are reviewed at least once daily: all security events, logs of all system components that store, process, or transmit Cardholder Data (hereinafter – "CHD") and/or Sensitive Authentication Data (hereinafter – "SAD"), logs of all critical system components, logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (hereinafter – "IDS/IPS"), authentication servers).
- Logs of all other system components are reviewed periodically.
- Exceptions and anomalies identified during the review process are addressed.

10.5 Audit log history is retained and available for analysis. Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

- System clocks and time are synchronized using time-synchronization technology.
- Systems are configured to the correct and consistent time as follows:
    - One or more designated time servers are in use.
    - Only the designated central time server(s) receives time from external sources.
    - Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC).

DRAFT - LEGAL REVIEW REQUIRED

- The designated time server(s) accept time updates only from specific industry-accepted external sources.
- Where there is more than one designated time server, the time servers peer with one another to keep accurate time.
- Internal systems receive time information only from designated central time server(s).

- Time synchronization settings and data are protected as follows:
  - Access to time data is restricted to only personnel with a business need.
  - Any changes to time settings on critical systems are logged, monitored, and reviewed.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

- Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:
  - Network security controls.
  - IDS/IPS.
  - File Integrity Monitoring (hereinafter – "FIM").
  - Anti-malware solutions.
  - Physical access controls.
  - Logical access controls.
  - Audit logging mechanisms.
  - Segmentation controls (if used).
- Failures of any critical security control systems are responded to promptly, including but not limited to:
  - Restoring security functions.
  - Identifying and documenting the duration (date and time from start to end) of the security failure.
  - Identifying and documenting the cause(s) of failure and documenting required remediation.
  - Identifying and addressing any security issues that arose during the failure.
  - Determining whether further actions are required as a result of the security failure.
  - Implementing controls to prevent the cause of failure from reoccurring.
  - Resuming monitoring of security controls.

11. REQUIREMENT 11: TEST SECURITY OF SYSTEMS AND NETWORKS REGULARLY

11.1 All security policies and operational procedures are defined and understood.

DRAFT - LEGAL REVIEW REQUIRED

The company maintains a set of documented security policies and operational procedures.

Roles and responsibilities for all security policies and operational procedures are assigned and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

- Authorized and unauthorized wireless access points are managed as follows:
  - The presence of wireless (Wi-Fi) access points is tested for,
  - All authorized and unauthorized wireless access points are detected and identified,
  - Testing, detection, and identification occurs at least once every three months.
  - If automated monitoring is used, personnel are notified via generated alerts.
- An inventory of authorized wireless access points is maintained, including a documented business justification.

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

- Internal vulnerability scans are performed as follows:
  - At least once every three months.
  - Vulnerabilities that are either high-risk or critical are resolved.
  - Rescans are performed that confirm all high-risk and all critical vulnerabilities (as noted above) have been resolved.
  - Scan tool is kept up to date with latest vulnerability information.
  - Scans are performed by qualified personnel and organizational independence of the tester exists.
- External vulnerability scans are performed as follows:
  - At least once every three months.
  - By a PCI SSC Approved Scanning Vendor (hereinafter – "ASV").
  - Vulnerabilities are resolved and ASV Program
  - Guide requirements for a passing scan are met.
  - Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

- A penetration testing methodology is defined, documented, and implemented by the entity, and includes:
  - Industry-accepted penetration testing approaches.
  - Coverage for the entire CDE perimeter and critical systems.
  - Testing from both inside and outside the network.
  - Testing to validate any segmentation and scope- reduction controls.

DRAFT - LEGAL REVIEW REQUIRED

    - Application-layer penetration testing to identify.
    - Network-layer penetration tests that encompass all components that support network functions as well as operating systems.
    - Review and consideration of threats and vulnerabilities experienced in the last 12 months.
    - Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.
    - Retention of penetration testing results and remediation activities results for at least 12 months.
- Internal penetration testing is performed.
    - Per the entity's defined methodology,
    - At least once every 12 months
    - After any significant infrastructure or application upgrade or change
    - By a qualified internal resource or qualified external third-party
    - Organizational independence of the tester exists (not required to be a QSA or ASV).
- External penetration testing is performed:
    - Per the entity's defined methodology
    - At least once every 12 months
    - After any significant infrastructure or application upgrade or change
    - By a qualified internal resource or qualified external third party
    - Organizational independence of the tester exists (not required to be a QSA or ASV)
- Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows:
    - In accordance with the entity's assessment of the risk posed by the security issue.
    - Penetration testing is repeated to verify the corrections.
- If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:
    - At least once every 12 months and after any changes to segmentation controls/methods
    - Covering all segmentation controls/methods in use.
    - According to the entity's defined penetration testing methodology.
    - Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
    - Confirming effectiveness of any use of isolation to separate systems with differing security levels.

DRAFT - LEGAL REVIEW REQUIRED

- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

- If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:
  - At least once every six months and after any changes to segmentation controls/methods.
  - Covering all segmentation controls/methods in use.
  - According to the entity's defined penetration testing methodology.
  - Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
  - Confirming effectiveness of any use of isolation to separate systems with differing security levels.
  - Performed by a qualified internal resource or qualified external third party.
  - Organizational independence of the tester exists (not required to be a QSA or ASV).

11.5 Network intrusions and unexpected file changes are detected and responded to.

- Intrusion-detection and/or intrusion- prevention techniques are used to detect and/or prevent intrusions into the network as follows:
  - All traffic is monitored at the perimeter of the CDE.
  - All traffic is monitored at critical points in the CDE.
  - Personnel are alerted to suspected compromises.
  - All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.
- A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows:
  - To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files.
  - To perform critical file comparisons at least once weekly.

11.6 Unauthorized changes on payment pages are detected and responded to.

12. REQUIREMENT 12: SUPPORT INFORMATION SECURITY WITH ORGANIZATIONAL POLICIES AND PROGRAMS

12.1 Support information security with organizational policies and programs are defined and understood.

The company maintains a set of documented support information security with organizational policies and programs.

DRAFT - LEGAL REVIEW REQUIRED

Roles and responsibilities for support information security with organizational policies and programs are assigned and understood.

12.2 Acceptable use policies for end-user technologies are defined and implemented. Acceptable use policies for end-user technologies are documented and implemented, including:

- Explicit approval by authorized parties.
- Acceptable uses of the technology.
- List of products approved by the company for employee use, including hardware and software.

12.3 Risks to the CDE are formally identified, evaluated, and managed.

- For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes:
    - Identification of the assets being protected.
    - Identification of the threat(s) that the requirement is protecting against.
    - Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
    - Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized.
    - Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
    - Performance of updated risk analyses when needed, as determined by the annual review.
- A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include:
    - Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis).
    - Approval of documented evidence by senior management.
    - Performance of the targeted analysis of risk at least once every 12 months.

12.4 PCI DSS compliance is managed.

- Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include:
    - Overall accountability for maintaining PCI DSS compliance.
    - Defining a charter for a PCI DSS compliance program and communication to executive management.
- Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks:

DRAFT - LEGAL REVIEW REQUIRED

- Daily log reviews.
- Configuration reviews for network security controls.
- Applying configuration standards to new systems.
- Responding to security alerts.
- Change-management processes.

12.5 PCI DSS scope is documented and validated.

- An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.
- PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes:
  - Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card- present, card-not-present, and e-commerce).
  - Updating all data-flow diagrams.
  - Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.
  - Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.
  - Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.
  - Identifying all connections from third-party entities with access to the CDE.
  - Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.

12.6 Security awareness education is an ongoing activity.

- A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.
- Personnel receive security awareness training as follows:
  - Upon hire and at least once every 12 months.
  - Multiple methods of communication are used.
  - Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.

12.7 Personnel are screened to reduce risks from insider threats. Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.

DRAFT - LEGAL REVIEW REQUIRED

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

- A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.
- Written agreements with TPSPs are maintained as follows:
    - Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.
    - Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data.
- An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.
- A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.
- Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.

12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

- TPSPs provide written agreements to customers that include acknowledgments that TPSPs are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that the TPSP could impact the security of the customer's cardholder data and/or sensitive authentication data.
- TPSPs support their customers' requests for information by providing the following upon customer request:
    - PCI DSS compliance status information.
    - Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities, for any service the TPSP provides that meets a PCI DSS requirement(s) on behalf of customers or that can impact security of customers' cardholder data or sensitive authentication data.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

- An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:
    - Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
    - Incident response procedures with specific containment and mitigation activities for different types of incidents.

DRAFT - LEGAL REVIEW REQUIRED

    - Business recovery and continuity procedures.
    - Data backup processes.
    - Analysis of legal requirements for reporting compromises.
    - Coverage and responses of all critical system components.
    - Reference or inclusion of incident response procedures from the payment brands.
- At least once every 12 months, the security incident response plan is:
    - Reviewed and the content is updated as needed.
    - Tested.
- Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.
- Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.
- The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:
    - Intrusion-detection and intrusion-prevention systems.
    - Network security controls.
    - Change-detection mechanisms for critical files.
    - The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
    - Detection of unauthorized wireless access points.
- The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.

DRAFT - LEGAL REVIEW REQUIRED

AUDIT PROCEDURE POLICY

1. SCOPE AND PURPOSE OF AUDITS

The Controller is entitled to conduct audits to verify the Processor's compliance with the GDPR, this Agreement, and the applicable provisions of the SCC. The audits may include:

- Reviewing documentation and records related to data processing activities.
- Evaluating the effectiveness of technical and organizational measures implemented to ensure data protection.
- Assessing compliance with agreed-upon policies, including data security, access control, and incident management.

2. LIMITATIONS ON AUDIT ACCESS

To ensure security and confidentiality:

- **The Processor will not provide physical access to data centers where its equipment and infrastructure are located.**
- Instead, the Processor shall provide sufficient documentation, certifications (e.g., ISO 27001, PCI DSS).
- Virtual audits, including video conferences and shared access to audit logs, may be conducted as agreed upon by the Parties.

3. NOTIFICATION AND PLANNING

- The Controller shall notify the Processor of the intent to conduct an audit at least 30 calendar days in advance.
- The scope, duration, and specific objectives of the audit shall be agreed upon in writing by both Parties prior to the commencement of the audit.
- Audits shall be conducted during normal business hours and in a manner that minimizes disruption to the Processor's operations.

4. COSTS OF AUDITS

- The Processor shall be compensated for time spent by its employees in cooperating with the audit. The Controller agrees to pay a fee of 150 EUR per hour for such cooperation.
- An estimate of expected costs will be provided by the Processor prior to the audit, based on the agreed scope and duration. The Controller shall confirm acceptance of these costs in writing before the audit begins.

DRAFT - LEGAL REVIEW REQUIRED

5. CONFIDENTIALITY AND DATA PROTECTION

- The Controller shall treat all information obtained during the audit as confidential and use it solely for the purposes of ensuring compliance with GDPR and the Agreement.
- Any data accessed during the audit must not be copied, retained, or used beyond the scope of the audit.

6. AUDIT FREQUENCY

- Audits may be conducted no more than once per calendar year unless there are reasonable grounds to suspect a breach of the Processor's obligations.
- Relevant certifications and third-party audit reports may be used to satisfy the Controller's audit requirements, reducing the need for an on-site or extensive audit.

7. POST-AUDIT ACTIONS

- The Controller shall provide a report of findings to the Processor within 30 days of completing the audit.
- The Processor shall address any identified non-compliance within a mutually agreed timeframe.

DRAFT - LEGAL REVIEW REQUIRED

Annex IV

LIST OF SUB-PROCESSORS

#	Sub-Processor Name	Location	Purpose of Processing	Data Categories Processed	Safeguards/Certifications
1.	----------	----------	----------	----------	----------

DRAFT - LEGAL REVIEW REQUIRED

ADDITIONAL ELEMENTS
FOR COMPLIANCE WITH ARTICLES 33 AND 34 GDPR

This Annex outlines the specific elements and procedures to be followed by the Processor in the event of a personal data breach, as required under Articles 33 and 34 of GDPR. It ensures that the Processor provides the Controller with the necessary information and support to fulfill its legal obligations, including timely notification to supervisory authorities and, where applicable, affected data subjects.

The provisions of this Annex are intended to facilitate transparent communication, effective mitigation of risks, and compliance with all applicable legal requirements in the event of a breach. The Processor shall adhere to the requirements set forth herein to ensure a collaborative and effective response to any security incidents involving personal data.

1. INCIDENT DESCRIPTION

The Processor shall provide the following details about the personal data breach:

- **Nature of the breach**: A detailed description of the type of breach (e.g., unauthorized access, data loss, data corruption).
- **Categories and approximate number of data subjects concerned**: The groups of individuals affected (e.g., customers, employees) and an estimated count.
- **Approximate number of personal data records concerned**: An estimate of the number of records affected by the breach.

2. DETECTION AND TIMELINE

- **Date and time the breach was detected**: Information about when the breach was first identified by the Processor.
- **Duration of the breach**: The period during which the breach occurred, including the start and end times if known.

3. POINT OF CONTACT

The Processor shall designate a contact person for all communications regarding the breach.

4. LIKELY CONSEQUENCES

An analysis of the potential risks to data subjects resulting from the breach, including:

- Possible material damage, identity theft, or reputational harm.
- Other relevant impacts based on the nature of the breached data.

5. MEASURES TAKEN

The Processor shall detail the actions undertaken to address the breach, including:

DRAFT - LEGAL REVIEW REQUIRED

- **Immediate measures**: Actions to mitigate damage, such as restricting access, patching vulnerabilities, or isolating systems.
- **Long-term measures**: Steps to prevent future breaches, such as policy updates or system improvements.

6. NOTIFICATION ACTIONS

- **Status of notifications to supervisory authorities**: Indicate whether the breach has been reported to the relevant supervisory authority, including the date and content of the notification.
- **Status of notifications to data subjects**: Provide details on whether affected individuals have been informed, including how and when.

7. INCIDENT LOG ACCESS

The Processor shall maintain and provide access to an incident log, containing records of all actions taken to identify, mitigate, and resolve the breach.

8. RECOMMENDATIONS TO THE CONTROLLER

The Processor shall offer recommendations to the Controller, including:

- Suggested actions to further mitigate risks.
- Guidance on notifications to affected data subjects and supervisory authorities, if applicable.

9. CONTINUOUS SUPPORT

The Processor commits to providing ongoing assistance to the Controller during the breach resolution process, ensuring compliance with GDPR obligations.

DRAFT - LEGAL REVIEW REQUIRED