

January 2021

Data Processing Addendum

THIS ADDENDUM is deemed to be effective on the date of execution of the Merchant Services Agreement (the “**Agreement**”) between the **Merchant** (as defined therein) and **Credorax** (as defined therein), hereinafter collectively referred to as the "Parties"

Whereas, the parties have entered into the Agreement whereby Credorax shall provide the Merchant with certain Services (as defined therein); and

Whereas, in the course of providing the Service Credorax shall receive or have access to personal data collected by or on behalf of the Merchant; and

Whereas, in accordance with the requirements of applicable data protection legislation, the Parties wish to set forth the terms governing the processing by Credorax of such personal data.

Whereas, this Addendum will be effective, subject that no other written data processing addendum was signed by both Parties prior to this Addendum.

This Addendum defines the data processing relationship between the Parties and sets out the additional terms, requirements and conditions on which Credorax will process personal data for and on behalf of the Merchant when providing services under the Agreement. This Addendum contains the mandatory clauses required by Article 28(3) of the GDPR for contracts between controllers and processors

Now therefore, the Parties have agreed as follows:

Definitions

The following capitalized terms shall bear the meaning ascribed thereto. Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

"Addendum" shall mean this addendum in its entirety, including all schedules and annexes thereto, as the same may be amended from time to time.

“AML” means anti-money laundering.

“AML/KYC documentation” means any and all data or documentation that is required in order to satisfy and AML legal obligations.

"Controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the Controller (or the criteria for nominating the Controller) may be designated by those laws.

"Data Breach" shall mean breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed

“Data Protection Laws” shall mean (i) all Maltese Data Protection Legislation; (ii) any other EU legislation relating to personal data; and (iii) all other legislation and regulatory requirements in force from time to time which apply to a Party relating to the use of personal data (including without limitation, the privacy of electronic communications); and (iv) the guidance and codes of practice issued by the relevant data protection or supervisory authority and applicable to a Party; in each case as may be amended, supplemented or replaced from time to time;

"Data Subject" shall have the same meaning as that ascribed to it under Data Protection Laws

"GDPR" shall mean General Data Protection Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data as in force as amended, replaced or superseded from time to time, including any laws implementing or supplementing GDPR.

“Maltese Data Protection Law” means all applicable data protection on privacy legislation in force from time to time in Malta, including (i) the Data Protection act, Chapter 586 of the Laws of Malta; (ii) the GDPR; (iii) all national implementing laws, regulations and secondary legislation applicable in Malta which relate to the processing of personal data, in each case as may be amended, supplemented or replaced from time to time;

"Merchant Data" shall mean any Personal Data provided to Credorax by the Merchant or on its behalf or to which Credorax obtains access solely as a result of, or in connection with, the provision of the Services;

January 2021

"Personal Data" shall have the meaning set out in the GDPR.

"Privacy and Data Protection Requirements" shall refer Data Protection Legislation relating to the processing of personal data and privacy in any relevant jurisdiction, and any orders, guidelines and instructions issued under the relevant Supervisory Authority in Malta or the European Union.

"Processor" shall mean a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Merchant.

"Services" means the services as outlined and indicated in the Agreement.

Standard Contractual Clauses (SCC) shall mean the European Commission's Standard Contractual Clauses for the transfer of personal data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU (such clauses being incorporated in Annex A), as may be mended or replaced by the European Commission from time to time

"Sub-Processor" shall mean a natural or legal person, public authority, agency or any other body contracted by the Processor to process Personal Data for the purpose of carrying out a specific processing activity on behalf of the Controller in connection with the Services.

"Supervisory Authority" means the relevant supervisory authority established by a Member State pursuant to Article 51 of GDPR.

General

1. Both Parties warrant that they will comply with their respective obligations under Data Protection Laws and the terms of this Addendum. As between the Parties, it is hereby agreed that with regard to Merchant Data for the purposes of all Data Protection Laws, the Merchant shall act as Controller and Credorax shall act as Processor.
2. Subject to the provisions of the Agreement and any instruction that may be given from time to time in writing by the Merchant, Credorax is hereby appointed by the Merchant to process Merchant Data on behalf of the Merchant solely for the purpose of performing and fulfilling the Services as outlined in the Agreement (which, by and large, consists of the provision of acquiring

services, which include, but is not limited to, the processing and settlement of payment card Transactions according to regulatory and Card Scheme standards and requirements).

3. The Parties therefore acknowledge and agree that subject to Clause 9 of the Agreement (Data Protection and Privacy) the Merchant at all times, retains control of the Merchant Data and as the Controller, remains solely responsible for ensuring and maintaining compliance with any and all obligations which may be imposed upon Controllers of personal data under Data Protection Laws. This includes providing any required notices and mandatory information, and obtaining any required consents from data subjects, and for any and all instructions which it may give from time to time:

Merchant Obligations

The Merchant warrants and represents to Credorax that:

1. it shall be exclusively responsible for ensuring that it complies at all times with any and all obligations which it may have as the Controller of the relevant data under this Addendum and under the Data Protection Laws, and that all Personal and Merchant Data which it processes or gives access to;
2. all Merchant Data is obtained in accordance with Data Protection Laws and in particular, that where it has relied on consent as a means of processing personal data, it has obtained valid consent of the Data Subjects as required in terms of Data Protection Laws;
3. All instructions given to Credorax in terms of this Addendum and the Agreement shall at all times be in accordance with Data Protection Laws, and that the compliance, performance or execution of any and all such instructions will not, at any point in time, cause Credorax to be in breach of any Data Protection Laws;
4. It has provided the Data Subjects with all necessary information about the Processing of the Personal Data in the context of the Agreement as required by Data Protection Laws, including without limitation, information relating to the appointment of Processors transferring to, and processing personal information by, third parties which may retain or use the personal information for compliance with legal and regulatory requirements;
5. It shall maintain all necessary policies and processes to authorise the access and processing of the relevant data in the full manner contemplated by this Addendum and the Agreement;
6. The Merchant acknowledges that as Controller, it is solely responsible for determining the lawful processing condition upon which it shall rely in providing instructions to Credorax to process Merchant Data for the purposes of carrying out the Services as set out in the Agreement and that it shall stipulate what this lawful process is to the Processor.

Credorax Obligations

1. Credorax shall only carry out processing of Personal Data in accordance with the written instructions provided by the Merchant and only process same for the performance of the Services, including where relevant for transfers of EEA resident Personal Data outside the EEA or to an international organisation (unless Credorax is otherwise required to process Controller Data by European Union, Member State and/or Maltese law or any regulatory bodies to which Credorax is subject, in which case Credorax shall inform the Controller of that legal requirement unless prohibited by that law on grounds of public interest), and shall immediately inform the Merchant if, in the opinion of Credorax, any instruction given by the Merchant to Credorax infringes Data Protection Laws.
2. Credorax shall comply with its obligations as Processor under the relevant Data Protection Laws.
3. Credorax shall reasonably cooperate with Merchant with fulfilling Merchant's obligations as Controller in respect of Data Subject rights under the Data Protection Laws, including responding to any subject access requests or requests from Data Subjects for access to, rectification, erasure or portability of Personal Data, or for restriction of processing or objections to processing of Personal Data.
4. Credorax shall take all technical and security measures required pursuant to Article 32 of the GDPR.
5. where relevant for the processing of Personal Data provided by the Merchant and taking into account the nature of the processing and the information available to Credorax, use all measures to assist the Merchant in ensuring compliance with the obligations of the Merchant to; (i) keep Personal Data secure at all times; (ii) implement and maintain appropriate technical and organization measures to protect against unauthorized or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of the Personal Data and against accidental or unlawful loss, destruction alteration, disclosure or damage to the Personal data, including but not limited to, the security measures as set out in the Agreement. Credorax shall document such measures in writing and periodically review them to ensure they remain current and complete
6. In case of a Data Breach, Credorax shall immediately, and in any case within 36 hours of becoming aware, inform the Merchant of any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access or any other form of unauthorized

processing, or of any disruptions endangering the security of the Data Subject's Personal 'Data, or Merchant Data transmitted, stored or otherwise processed. Credorax accepts and acknowledges that the Merchant shall direct in its sole discretion, any and all steps and measures taken to remedy a breach by Credorax under Data Protection Laws, including but not limited to any communications with a Supervisory Authority, unless otherwise required by law. Credorax agrees not to act in any way upon such disclosure without the prior written consent of the Merchant, unless otherwise required by law.

7. On expiry or termination of the Agreement, Credorax shall immediately cease to use Merchant Data and shall arrange for its safe return or destruction as shall be required by the Merchant (unless European Union, Member State and/or Maltese Law requires storage of any Merchant Data. or an exemption under GDPR applies).
8. Credorax shall make available to the Merchant all information necessary to demonstrate compliance with the obligations under Data Protection Laws and allow for and contribute to audits, including inspections, conducted by the Merchant or another auditor mandated by the Merchant .
9. Credorax shall assist the Merchant in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR taking into account the nature of processing and the information available to Credorax.

Audit Rights

1. Upon the Merchant's reasonable prior written request, Credorax agrees to provide the Merchant with any documentation or records (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) which will enable it to verify and monitor Credorax's compliance with its data protection and security obligations under the terms of this Addendum. Credorax shall provide such information within sixty (60) days of receipt of such request, and notify the Merchant of the person within Credorax's organization who will act as the point of contact for provision of the information required by the Merchant. Any costs incurred with respect to an audit will be borne by the Merchant, depending on the effort estimated by Credorax.
2. Where, in the reasonable opinion of the Merchant, such documentation is not sufficient in order to meet the obligations of Article 28 of the GDPR, the Merchant will be entitled, upon providing 30 days prior written notice to Credorax and upon reasonable grounds, to conduct an on-site audit of Credorax's premises used in connection with the Service, solely to confirm compliance with its

data protection and security obligations under this Addendum. Any such audit will be limited in time and shall last no longer than 3 business days, during business hours.

3. Any audit carried out by the Merchant will be conducted in a manner that does not disrupt, delay or interfere with Credorax's performance of its business. The Merchant shall ensure that the individuals carrying out the audit are under the same confidentiality obligations as set out in the Agreement. Any costs incurred with respect to such an audit will be borne by the Merchant.
4. Any audit right granted to Credorax under the Agreement shall remain in full force and effect. In the event that there is no audit right in favour of Credorax or the audit right contained in the Agreement in favour of Credorax is not sufficient to enable it to verify and monitor the Merchant's compliance with its data protection and security obligations under the terms of this Addendum, then, Credorax shall be entitled to carry out an audit of the Merchant on reciprocal terms as those set out in this clause 6.

Use of Sub-Processors

1. The Merchant hereby authorises and grants Credorax a general written authorization to appoint (and permit each Sub-Processor appointed in accordance with this provision to appoint) Sub processors in accordance with this provision and any restrictions contain in the Agreement.
2. Credorax shall notify the Merchant of any intended changes concerning the addition or replacement of Sub Processors, thereby giving the Merchant the opportunity to object to such changes. In the event of an objection, Credorax shall not appoint (nor disclose any Merchant Data) to the proposed Sub processor except with the prior written consent of the Merchant.
3. Credorax warrants and undertakes to, at all times, exercise direct responsibility and supervision over all Personal Data which it may entrust to a Sub-Processor in accordance with the preceding clause. Credorax shall, at all times, remain fully liable to the Merchant in the event that the Sub-Processor fails to fulfil its data protection obligations and for all other actions and omissions of the Sub-Processor.
4. Credorax shall bind any and all Sub-Processors, validly appointed by Credorax in terms of this Clause by means of a written contract that contains processing clauses and obligations substantially the same as those set out and imposed in this Addendum and which (written contract) is stipulated to terminate automatically on expiry or termination of this Addendum for any reason

Credorax's Employee's

1. Credorax shall ensure that all employees and other personnel who are given access to the Merchant Data are adequately and responsibly informed of the confidential nature of the Personal Data and have committed themselves to confidentiality or are under appropriate statutory obligations of confidentiality.
2. Furthermore, such employees shall be aware of Credorax's duties and their personal duties and obligations under the relevant Data Protection Laws and this Addendum.

International Transfers of Personal Data

1. The Parties hereby agree that Credorax may transfer personal outside the EEA (a) on the basis of an adequacy decision; or (b) subject to appropriate safeguards, both as contemplated under GDPR.
2. In relation to point (b) above, namely transfers of personal data subject to adequate safeguards, the Merchant (acting as data exporter) hereby grants a non-revocable general mandate for Credorax to enter into and sign Standard Contractual Clauses for and on its behalf as Controller with any Sub-Processors (acting as data importers) located outside the EEA, annexed to this Agreement as Annex A.
3. In the interest of clarity, the Standard Contractual Clauses contained in Annex A are an integral part of this Agreement and the Merchant hereby acknowledges and agrees to the information contained in Appendices 1 and 2 of the Standard Contractual Clauses.
4. Subject to the above, where Personal Data originating in the EEA is processed by the Processor outside the EEA and in a territory that has not been designated by the European Commission as ensuring an adequate level of protection to data subjects (**adequacy decision**), the Processor and the Controller agree that the transfer between of such personal data either between the Processor and the Controller or alternatively, the Processor and any Sub-Processor shall be subject to the Standard Contractual Clauses which shall be deemed to apply in respect of any and all such processing carried out by the Processor outside the EEA.

Security

1. For the avoidance of doubt, both Parties acknowledge that any provisions in relation to PCI-DS Standards used in connection with the Credorax Services under the Agreement shall remain unchanged and in full force and effect.

2. Both parties warrant and agree that each shall carry out and implement any security measures (technical and organisation) which may be necessary or otherwise mandated under Data Protection Laws (specifically with respect to article 32 of the GDPR) to safeguard the privacy and security of the Personal and Merchant Data, and that these measure shall remain in place for the duration of the Agreement. This will include ensuring that there are sufficient technical and organisational measures to ensure data protection by default and by design.

Liability & Indemnity

Subject to the liability clauses in the Agreement, the Parties agree that they will be held liable for violations of EU Data Protection Law towards Data Subjects as follows:

1. The Merchant shall be liable for the damage caused by the processing of Merchant Data which infringes EU Data Protection Law or this Addendum only where it has not complied with obligations of EU Data Protection Law specifically directed to Controllers.
2. Credorax shall be liable for the damage caused by the processing of Merchant Data which infringes Data Protection Law or this Addendum only where it has not complied with obligations of Data Protection Law specifically directed to Processors or where it has acted in breach of its obligations under this Agreement. In that context, Credorax as Processor will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.
3. The Merchant shall indemnify, defend, and hold Credorax harmless from and against any and all claims, actions, suits, demands, assessments, or judgments asserted, and any and all losses, liabilities, damages, costs, and expenses (including, without limitation, attorneys fees, accounting fees, and investigation costs to the extent permitted by law) alleged or incurred arising out of or relating to any operations, acts, or omissions of the indemnifying party or any of its employees, agents, and invitees in the exercise of the indemnifying party's rights or the performance or observance of the indemnifying party's obligations under this agreement. Prompt notice must be given of any claim, and the Controller providing the indemnification will have control of any defence or settlement.

Applicable Law and Jurisdiction

This Clause is subject to the conditions stipulated in reciprocal clause in the Agreement.

Notice

January 2021

Any notice or other communication relating directly to this Addendum are to be given in writing to DPO@Credorax.com. This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

Miscellaneous

Where applicable, the Parties agree that if, upon review following GDPR coming into force, the provisions of this Data Processing Addendum do not comply with GDPR then both Parties agree to cooperate in good faith to renegotiate the terms of this Data Processing Addendum to ensure compliance with GDPR.

The Parties hereto have caused this Addendum to be duly accepted and executed by executing the Agreement.

January 2021

Annex A – Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

(DATA CONTROLLER TO DATA PROCESSOR)

Data transfer agreement

Credorax Bank Limited, a company registered and existing under the laws of Malta, bearing company registration number C46342 and having its registered address at Palazzo Homedes, 80 Strait Street, Valletta VLT 1436, Malta

as duly authorised to act for and on behalf of the Merchant

hereinafter “**data exporter**”

And

[Sub-Processor]

hereinafter “**data importer**”

each a “Party”; collectively “the Parties”.

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Definitions

For the purposes of the Clauses:

- (a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

- (b) 'the data exporter' means the controller who transfers the personal data
- (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity

has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing

services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer¹

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

¹ Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its

January 2021

rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Indemnification

1. The data importer agrees that if it is held liable for a violation of the clauses committed bit shall indemnify the data exporter for any cost, charge, damages, expenses or loss it has incurred.
2. Indemnification is contingent upon:
 - (a) the data exporter promptly notifying the data importer of a claim; and
 - (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim

Clause 8

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established (Malta).
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 9

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant

to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 10

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the Laws of Malta.

Clause 11

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 12

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses². Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the laws of Malta.

² This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

January 2021

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 13

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

January 2021

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Transferring personal data for the provision of services as detailed in the

Agreement.....

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Processing personal data to enable and facilitate the provision of the services detailed in the

Agreement.....

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Cardholders or shoppers of the Controller; Management personnel of the Controller

Categories of data

The personal data transferred concern the following categories of data (please specify):

Encrypted credit card number, name, email, address, IP address and any other information transferred by the controller;

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

.....N/A.....

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):
processing, storing, analyzing, visualizing, and monitoring data

DATA EXPORTER

Name:.....

Authorised Signature

DATA IMPORTER

Name:.....

Authorised Signature

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Data encryption as required by applicable by the relevant PCI standards

Compliance program

January 2021