PBZ Card d.o.o. having its principal place of business at Radnička cesta 44, 10000, Zagreb (the "Licensee", the „Controller")

and

Thomalex, Inc., a Florida company having its principal place of business at 1920 E Hallandale Beach Blvd, Suite 907, Hallandale Beach, FL 33009, United States (the "Licensor", the „Processor")

Licensee and Licensor together as „Parties"

have entered into

DATA PROCESSING ADDENDUM

I. INTRODUCTION

Clause 1.

This Data Processing Addendum ("DPA") is incorporated into, and is subject to the terms and conditions of the Software End User License Agreement of 7.2.2022(date of the Agreement). between the Licensor and the Licensee.

Contracting parties hereby acknowledge and agree that with regard to the processing of personal data, Licensee is the controller and Licensor is a processor acting on behalf of Licensee. For the avoidance of doubt, this DPA shall not apply to instances where Licensor is the controller (as defined in the applicable Data Protection Laws).

Considering that the Licensor as a processor of personal data is a company having its principal place of business in the United States of America and that the European Commission has decided under article 45 (5) of the Directive 95/46/EC (General Data Protection Regulation) (hereinafter: GDPR) that United States of America no longer provide an adequate level of protection of personal data, the Contracting parties are making this DPA in accordance with article 46 (2) of GDPR and in accordance with the Commission implementing deThomalex (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: standard contractual clauses). For the purpose of harmonizing wording with standard contractual clauses, Parties hereby determine that Licensee (controller) is an importer and Licensor (processor) is an exporter of personal data.

II. PURPOSE AND SCOPE

Clause 2.

(a)The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)(1) for the transfer of personal data to a third country.

(b) These Clauses apply with respect to the transfer of personal data as specified in Annex I.

(c)The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 3.

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the processor and/or controller.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4.

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5.

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6.

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.

Clause 7.

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or data importer, controller or processor by completing and signing the Appendix.

(b) Once it has completed and signed the Appendix, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer, controller or processor in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8.

8.1 Instructions

(a) The processor shall process the personal data only according to this Agreement, Thomalex Leisure Solution Agreement with PBZ Card d.o.o (main contract) and instructions from the controller.

(b) The processor shall immediately inform the controller if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The processor shall refrain from any action that would prevent the controller from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return to the controller all personal data processed on its behalf and delete existing copies.

8.2. Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal dana, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The processor shall assist the controller in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the processor under these Clauses, the processor shall notify the controller without undue delay after becoming aware of it and assist the controller in addressing the breach.

(c) The processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall make available to the controller all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9.

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the controller or, for data processing by the processor in the EU, under Regulation (EU) 2016/679.

Clause 10.

(a) The Parties shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the Parties shall accept the deThomalex of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 12;

(ii) refer the dispute to the competent courts within the meaning of Clause 17.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The Parties shall abide by a deThomalex that is binding under the applicable EU or Member State law.

(f) The Parties agree that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 11.

(a) The processor shall be liable to the controller for any damages it causes to the controller by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the processor under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

Clause 12.

The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established is Croatian Personal Data Protection Agency., which shall act as competent supervisory authority.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 13.

(a) The processor warrants that has no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the processor, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the controller from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The processor declares that in providing the warranty in paragraph (a) has taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The processor warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the controller with relevant information and agrees that it will continue to cooperate with the controller in ensuring compliance with these Clauses.

(d) The processor agrees to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The processor agrees to notify the controller promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the controller otherwise has reason to believe that the processor can no longer fulfil its obligations under these Clauses, the controller shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the processor and/or controller to address the situation. The controller shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the controller shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the controller may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 15 (d) and (e) shall apply.

Clause 14.

14.1. Notification

(a) The processor agrees to notify the controller and, where possible, the data subject promptly (if necessary with the help of the controller) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the

request, the draft of the response for which they are required to obtain the prior consent of the controller and finally the approved response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the processor.

(b) If the processor is prohibited from notifying the controller and/or the data subject under the laws of the country of destination, the processor agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The processor agrees to document its best efforts in order to be able to demonstrate them on request of the controller.

(c) Where permissible under the laws of the country of destination, the processor agrees to provide the controller, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The processor agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the processor pursuant to Clause 13(e) and Clause 15 to inform the controller promptly where it is unable to comply with these Clauses.

14.2. Review of legality and data minimisation

(a) The processor agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The processor shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the processor shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 13(e).

(b) The processor agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the controller. It shall also make it available to the competent supervisory authority on request.

(c) The processor agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 15.

(a) The processor shall promptly inform the controller if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the processor is in breach of these Clauses or unable to comply with these Clauses, the controller shall suspend the transfer of personal data to the processor until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 13(f).

(c) The controller shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the controller has suspended the transfer of personal data to the processor pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the processor is in substantial or persistent breach of these Clauses; or

(iii) the processor fails to comply with a binding deThomalex of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the controller may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d) Personal data collected by the processor in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.

The processor shall certify the deletion of the data to the controller. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses. In case of local laws applicable to the processor that prohibit the return or deletion of the transferred personal data, the processor warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a deThomalex pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 16.

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Florida, United States.

Clause 17.

All disputes arising out of or in connection with the present contract shall be submitted to the International Court of Arbitration of the International Chamber of Commerce and shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said Rules.

THOMALEX, INC

By: Rastko Ilic

Signature: DocuSigned by: Rastko Ilic C4F21D21EE61497...

Title: Chief Executive Officer

Date: 2/8/2022

PBZ Card d.o.o

By: MISLAV BLAŽIĆ

Signature:

Title: PRESIDENT OF THE MANAGEMENT BOARD

Date:

PBZ Card d.o.o. Zagreb 2

ANNEX I

DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred.
   Data subjects who want to book and purchase an airplane ticket through Controller's website and bussines aplication of the Processor.

2. Categories of personal data transferred
   Name, surname, gender, date of birth, passport or ID number, passport or ID number validity,nationality,phone number, e-mail address, home address

3. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
   Data transfer is on continuous basis.

4. Nature and purpose of the data transfer and further processing
   The data is processed as follows:
   In the business applications of the Processor, data are collected, recorded, stored and sent to Controller for the purpose of booking and purchase of airplane ticket.
   Data processing is required for concluding and implementingpurchase contracts with data subjects.

5. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
   Personal data information must be deleted one year after data transfer.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

This document describes technical and organizational security measures and controls implemented by Thomalex, or Thomalex affiliates (hereafter Thomalex), to protect personal data and ensure the ongoing confidentiality, integrity and availability of Thomalex's products and services.

This document is a high-level overview of Thomalex's technical and organizational security measures. More details on the measures we implement are available upon request. Thomalex reserves the right to revise these technical and organizational measures at any time, without notice, so long as any such revisions will not materially reduce or weaken the protection provided for personal data that Thomalex processes in providing its various services. In the unlikely event that Thomalex does materially reduce its security, Thomalex shall notify its customers

Thomalex shall take the following technical and organizational security measures to protect personal data:

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of Thomalex's information security program.
2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to the Thomalex organization, monitoring and maintaining compliance with Thomalex policies and procedures, and reporting the condition of its information security and compliance to senior internal management.
3. Maintain Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them.
4. Communication with Thomalex applications utilizes cryptographic protocols such as TLS to protect information in transit over public networks. At the network edge, stateful firewalls, web application firewalls, and DDoS protection are used to filter attacks. Within the internal network, applications follow a multi-tiered model which provides the ability to apply security controls between each layer.
5. Data security controls which include logical segregation of data, restricted (e.g. role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.
6. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users,

periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

7. Password controls designed to manage and control password strength, and usage including prohibiting users from sharing passwords.
8. System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.
9. Physical and environmental security of data center, server room facilities and other areas containing client confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of Thomalex facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
10. Operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Thomalex possession.
11. Change management procedures and tracking mechanisms to designed to test, approve and monitor all changes to Thomalex technology and information assets.
12. Incident / problem management procedures designed to allow to Thomalex investigate, respond to, mitigate and notify of events related to Thomalex technology and information assets.
13. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
14. Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
15. Business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.
16. A Data Protection Officer (DPO) who is independent, regularly reviews data protection risks and controls.

ENGLISH	CROATIAN
I confirm that I am informed and aware of the fact that by continuing this process my personal data (name,surname,gender,date of birth,passport or ID number, passport or ID number validity, nationality, phone number, e-mail address, home address) will be processed in the USA, which country by decision of the European Commission under Article 45 (5) of Directive 95/46 / EC (GDPR) no longer provides an adequate level of personal data protection and that I have been informed of my right to obtain a copy of the standard contractual clauses and information about any onward transfer.	Potvrđujem da sam upoznat/a i svjestan/svjesna činjenice da će se nastavkom ovog procesa moji osobni podaci (ime, prezime, spol, datum rođenja broj putovnice ili osobne iskaznice, valjanost putnog dokumenta, broj telefona, e-mail i adresa) obrađivati u SAD-u, koja država odlukom Europske komisije prema članku 45. stavku 5. Direktive 95/46. / EC (GDPR) više ne pruža odgovarajuću razinu zaštite osobnih podataka i da sam obaviješten/a o svom pravu na dobivanje kopije standardnih ugovornih klauzula i informacija o svakom daljnjem prijenosu.
I confirm that it has been made available to me and that I have read the standard contractual clauses under Article 46 (2) of Directive 95/46 / EC (GDPR) and in accordance with Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council.	Potvrđujem da mi je stavljeno na raspolaganje i da sam pročitao/la standardne ugovorne klauzule prema članku 46. stavku 2. Direktive 95/46/EZ (GDPR) i u skladu s Provedbenom odlukom Komisije (EU) 2021/914 od 4. lipnja 2021. o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća.

Potvrdom oznake prihvata *Uvjeta usluge* korisnik potvrđuje da je pročitao, razumio i da prihvaća sve dokumente i izjave koje čine *Uvjete usluge.*