

Agreement

between

MUSEMENT S.p.A., whose registered office is at Via Polesine 13, 20139 Milan, Tax and VAT code IT07978000961, Milan Companies Registry MI-1995020 (hereinafter also referred to as MUSEMENT)

and

the Tour Operator, DMC, Transfer Company, Incoming Agency, Event Organizer, Licensed Tour Guide and/or Museum (hereinafter also referred to as the Supplier) identified in the <https://business.musement.com> web application each one referred to herein individually as a Party and collectively as the Parties.

Whereas

1. MUSEMENT – an authorized online travel agency – has developed a technological platform for the aggregation of online booking services mainly accessible through the www.musement.com portal and apps on various technological platforms, including Android and iOS (hereinafter the Portals), in addition MUSEMENT markets certain products related to leisure and travel also in physical venues and through third party resellers (the Retail Channels), which may also use their own trade name in connection with the sales under this agreement.
2. The Supplier, a company that is engaged principally in the business of developing, performing, managing, marketing and selling tourist, cultural and leisure services (hereinafter the Services), wishes to appoint MUSEMENT for the sale to the Portals' users and to the clients of the Retail Channels (hereinafter the Users) of vouchers or tickets granting the right to use the Services (hereinafter the "Products"),
3. The Supplier declares that it knows and accepts how the Portals work and the manner in which the Services and the Products are presented and promoted thereon,

the Recitals are an integral, essential and substantive part hereof,

NOW THEREFORE, the Parties agree as follows.

1. SUBJECT MATTER OF THE AGREEMENT

1.1. MUSEMENT undertakes to offer the Products in relation to the Services proposed by the Supplier for online or offline sale through the Portals, publishing thereon the information about the Services as furnished by the Supplier. The Supplier agrees that MUSEMENT can – at its own discretion – sell the Products also through the Retail Channels (including, but not limited to, travel agencies, sale points managed by MUSEMENT and third party resellers) publishing thereon the information about the Services as furnished by the Supplier, both under MUSEMENT trade name and/or other trademarks or trade names.^[SEP] Until all the places available for the relevant Service have been filled in the relevant day, the Supplier undertakes to provide MUSEMENT– on equal terms with other suppliers of Vouchers, including the Supplier – with the Products for their sale through the Portals and/or in the Retail Channels.

1.2. The Parties acknowledge that as at the date of signature of the Agreement, the provisions of this Agreement apply to the Supplier's Services specified in the information and material provided by the Supplier. The Parties agree that they may mutually agree to extend the provisions of this Agreement to further Services organised from time to time by the Supplier that are communicated to MUSEMENT, subject to acceptance by MUSEMENT.

1.3. MUSEMENT shall enjoy full technical, editorial and creative freedom in relation to every component of the Portals and (if applicable) other Retail Channels, and in relation to the terms and conditions of use thereof by the Users.^[SEP]

2. MUSEMENT'S OBLIGATIONS CONCERNING SALES

2.1. In the event a maximum overall selling price is agreed, MUSEMENT shall offer the Products for sale to the Users at an overall price which is not higher than this maximum overall selling price set by the Supplier.

2.2. MUSEMENT shall provide the User with the Products in the form of a voucher, ticket or applicable document reviewed by the Supplier, and the Supplier with the following data in relation to each Product sold: (a) city; (b) service purchased; (c) User's name and surname; (d) purchase/booking code; (e) date and time of commencement of use of the Service; (f) number of participants.

2.3. Should a User who has duly purchased a Product not be able to fully and timely enjoy the Service for any reason whatsoever attributable to the Supplier, or should the User (or any attendee) have been otherwise damaged in the use of the services offered by the Supplier, liability therefor and the burden of refunding the price of the Product and of compensating possible damages in favour of the User or third parties shall be borne exclusively by the Supplier.^[SEP]

3. MUSEMENT'S OBLIGATIONS CONCERNING PRESENTATION OF THE SERVICES

3.1. MUSEMENT undertakes to publish the information on each Service on a dedicated page of the Portals, and to display dedicated material on each Product and/or Service in any other Retail Channel, elaborating on the material furnished by the Supplier pursuant to article 5.1 below.

3.2. MUSEMENT assumes no obligation regarding the possible temporary or stable placement of information/banners relating to the Service on the home page (and/or other particular page and/or section) of the Portals, maintaining its total freedom in choosing all of the contents published thereon.^[SEP]

4. TECHNICAL AND OPERATING CHARACTERISTICS

4.1. The Supplier may access an online dashboard at the back-end of the page of the Portal reserved for its Services (hereinafter the "Account") by inserting a username and password (hereinafter the "Authentication Tools") at the <http://business.musement.com> webpage. Through the Account the Supplier's representative may check at any time all of the information indicated in article 2.2 above in relation to every Product sold.^[SEP] Knowledge of the Authentication Tools by third parties would allow them to access the Account and change the data therein contained. Therefore, the Supplier must keep the Authentication Tools totally confidential and use them with the utmost care. MUSEMENT shall not be held liable under any circumstances for any direct and/or indirect loss whatsoever arising out of the Supplier's failure to exhibit the care specified just now.

5. THE SUPPLIER'S OBLIGATIONS AND DUTIES

5.1. The Supplier undertakes to send MUSEMENT – within 5 (five) business days after the acceptance of the Agreement as regards the Services specified in the information and material provided by the Supplier and with not delay for any further Service that is subsequently covered by the Agreement – a sufficient amount of editorial content (including text, reviews, images and, where available, video) presenting each Service, in English and in any other language the Supplier might have available, and complying with the format and quality requirements from time to time specified by MUSEMENT. The

Supplier undertakes to update the material in question whenever it is necessary in order to provide the Users with clear and complete information on the Services.

5.2. By means of this Agreement and for the entire term hereof the Supplier grants MUSEMENT the right to copy and develop the material in question with full creative and editorial freedom in order to create (using the said material alone or in combination with other works) the pages of the presentation referred to in article 3.1 above for publication on the Portals and (if applicable) in the Retail Channels; and banners or other promotional material of the Services, the Supplier, the Portals and the Retail Channels that may be communicated to the public through Portals and/or the Retail Channels and/or any other means of communication without limit as time or territory.

5.3. The Supplier undertakes to notify MUSEMENT at least 7 (seven) business days in advance any temporary or permanent change to and/or limitation on the times and/or availability of the Services. Should use of the Service prove to be limited or precluded for unforeseeable reasons of force majeure, the Supplier shall immediately inform MUSEMENT so as to permit the latter to suspend the sale of the Vouchers and, where possible, to inform the purchaser of the impossibility to use the Service.

5.4. The Supplier will accept the Products presented by the Users both as paper print-outs or as electronic copies (in PDF or other equivalent formats) on smartphones or other electronic devices pertaining to the Users.^[SEP]

5.5. The Supplier undertakes to comply with the Information Security Schedule included in **Annex I**.

6. USE OF THE PARTIES' TRADEMARKS AND OTHER DISTINCTIVE SIGNS

6.1. For the entire term of Agreement, the Supplier grants to MUSEMENT a non-exclusive, royalty-free, worldwide and sub-licensable to third parties' right to use, publish, reproduce, distribute, display, making available to the public, broadcast, database, edit and modify the photographs and/or videos including images of recognizable persons and/or designs, logos, trademarks or other distinctive signs of the Supplier - whether individual or as part of it - plus any text provided to MUSEMENT (hereinafter, jointly referred to as the "Content") by any media (printed, digital, electronic, broadcast or otherwise, i.e. brochures, publications, the Portals and the Retail Channels, websites, marketing materials and electronic communications), on a permanent basis anywhere in the world, for commercial use, especially the offer and advertisement of products and services in the relevant territory. The Supplier further agree that the Licensee has the right, but not the obligation, to use the name and surname of the photographer/author in connection with the publication of the Content as reference for the copyright ["photo credit": for e.g. "© photo: Name Surname / company (agency)].

6.2. The Supplier represents and warrants that is and will continue to be the sole legal and beneficial owner or licensor of the right of use granted herein and has the necessary permissions to authorize the use of the Content. The Supplier further represents and warrants that the Content does not and will not infringe the copyright, the trademark rights or the design rights or other intellectual proprietary rights of any third party. The Supplier agrees to indemnify, defend and hold harmless MUSEMENT and its sublicensees against any and all losses, damages, expenses or costs including the costs involved for an appropriate legal defense incurred by MUSEMENT and/or its sublicensees arising from any claims, proceedings or actions by any third party based on the use of the licensed Content or intellectual property-rights by Licensee and/or sublicensees in connection with any goods and services in the event that the Content or intellectual property-rights (or any part thereof) infringes or is likely to infringe the intellectual property rights of any third party.

6.3. Wherever the Content includes personal image or voice, the Supplier represents and warrants that it has informed the owner of the image or voice with the relevant points included in the EU GDPR. Moreover, Supplier must ensure that it holds the pertinent consent from the Data subject. The Supplier

shall provide MUSEMENT with the written proof of such consent upon request. In case MUSEMENT would receive any complaint for the breach of the above representations, the Supplier will be the only liable and agrees to indemnify, defend and hold harmless MUSEMENT and its licensees against any such claims.

7. PRICES, FEES AND PAYMENTS

7.1. Without prejudice to MUSEMENT's right to set the selling price of the Products and to apply ancillary transaction fees at its own discretion (including prices lower than the Supplier Consideration in specific promotional periods), MUSEMENT undertakes to pay the Supplier the price/compensation which will be separately agreed by the Parties (hereinafter the "Supplier Consideration"). The Supplier Consideration for any price category (for example full or reduced vouchers): (a) shall include any applicable tax or charge; and (b) shall not be higher than the price applied to other resellers of the Products and/or by the Supplier at its premises.

7.2. The Supplier, with reference to each month of validity of this Agreement, shall issue an invoice to MUSEMENT that shall specify the overall amount of the Supplier Consideration accrued in the previous month minus the refunds and compensations made by MUSEMENT in favour of Users, if any. MUSEMENT shall pay the Supplier the Supplier Considerations, plus VAT (where applicable), out of payment charges, by the end of the month in which MUSEMENT has received a valid and correct invoice from the Supplier.

7.3. All of the invoices issued by Supplier to MUSEMENT shall be made out to Musement S.p.A. and sent to finance@musement.com.^[1]_[SEP]

8. MUSEMENT'S WARRANTIES AND SERVICE LEVELS

8.1. MUSEMENT undertakes to perform the services covered by this Agreement with the expertise expected of a professional operator.

8.2. Save as otherwise established by mandatory provisions of law for fraud or gross negligence, MUSEMENT shall not be liable for any direct or indirect loss of any nature and extent that may be suffered by the Supplier or third parties as a result of the use and/or failure to use the Portals, including in the case of delays or interruptions or by virtue of errors in and/or the malfunctioning of the Portals.^[1]_[SEP]

9. THE SUPPLIER'S WARRANTIES

9.1. The Supplier represents and warrants:

(a) That the Services will be accessible in the manner and at the times communicated to MUSEMENT pursuant to the Agreement, and will have the content described in the material furnished to MUSEMENT pursuant to article 5.1 above;

(b) That the material furnished to MUSEMENT pursuant to article 5.1 above is and will be correct and true, not breaching the personal and intellectual property rights of third parties;

(c) That it will bear all VAT (if payable), stamp duties and other taxes or deductions payable, on foot of the tax rules applicable from time to time, in connection with or relating in any way to the Products and the Services as well as to the collection of the price for the sale of Products and Services;

(d) That it is currently insured with a primary insurance institution against damages caused to third parties in the exercise of the Services.

9.2. The Supplier shall indemnify and hold MUSEMENT harmless against any claim, nuisance objection or demand by third parties that conflicts in any way with the warranties given above, and to this end at its own expense it shall take all appropriate action against those third parties and directly pay those third parties any sum that may be due to them in relation to the claims and nuisance in question, indemnifying and holding MUSEMENT harmless in respect of the costs, including unrecoverable ones, stemming from the said claims and nuisance.

9.3. Without prejudice to other remedies available to MUSEMENT based on the law and/or the Agreement, in case of breach of any of the provision of the Agreement by the Supplier, MUSEMENT shall have the right, at its own discretion, to withdraw any Supplier's Product or Service or content, to restrict the Supplier's use of the Portals, temporarily or permanently exclude (block) the Supplier from the Portals, or cancel existing bookings in the name of the Supplier without taking into account the applicable cancellation policies, and reject Users' offers for the conclusion of a purchase with the Supplier.

10. DATA PROTECTION

10.1 For the purpose of this Section, Data Protection Legislation means all applicable legislation and regulation relating to personal data, including Regulation (EU) 2016/679 and Directive 2002/58/EC, and mandatory guidance and codes of practice issued by the relevant supervisory authority and applicable to a party in force, as amended or replaced from time to time.

10.2 Each party shall determine the purposes and the means of their respective processing of personal data for the performance of this Agreement. Such processing shall not include providing personal data disclosed by TUI or on behalf of TUI ("TUI Data") to any third party unless otherwise required by any applicable law or court order. TUI shall retain all rights, title and interest in the TUI Data (including any amendments or alterations to the TUI Data).

10.3 Each party shall ensure that (a) it processes the personal data fairly, lawfully and in accordance with this Agreement and Data Protection Legislation; (b) it implements appropriate technical and organisational measures to ensure a level of data security appropriate to the risk; and (c) relevant employees have committed themselves to confidentiality and are trained to process personal data in accordance with Data Protection Legislation.

10.4 Unless prohibited by law, the parties shall without undue delay notify each other of any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data processed in connection with this Agreement ("Security Incident"). The parties shall provide all reasonable information, co-operation and assistance as is necessary to each other: (a) to minimise or stop such Security Incident; (b) to prevent such Security Incident reoccurring; and (c) to assist each other to comply with its internal/external reporting obligations.

11. TERM AND WITHDRAWAL

11.1. This Agreement is for an indefinite term commencing from the date of signature hereof. MUSEMENT and the Supplier agree that either of them may withdraw from this Agreement at any time by registered letter (with return receipt) giving notice of 60 (sixty) business days.^[L]_[SEP]

12. INTELLECTUAL PROPERTY RIGHTS

12.1. MUSEMENT and its predecessors in title are the exclusive owners of all of the intellectual property rights (including copyright) in all elements of the Portal, including the software that enables it to operate.^[L]_[SEP]

13. COMPLIANCE AND SUPPLY CHAIN

13.1 The Supplier and MUSEMENT agree to comply with all applicable laws, statutes, regulations and codes from time to time in force, including but not limited to, anti-corruption laws, international standards of compliance (collectively, the "Applicable Laws") and TUI's Supplier Code of Conduct, the Integrity Passport and the Human Rights Policy Statement as amended from time to time (together the "TUI Policies") which can be found on the TUI Group website (https://www.tuigroup.com/en-en/about-us/compliance/suppliers_code_of_conduct , <https://www.tuigroup.com/en-en/about-us/compliance>). The TUI Policies form an integral part of this Agreement.

13.2 The Supplier shall inform MUSEMENT of any violation of the Applicable Laws or the TUI Policies without undue delay.

13.3 The Supplier shall only enter into contracts with subcontractors in relation to the fulfilment of this Agreement upon execution of this Agreement and acceptance of the TUI Policies.

If required from a risk perspective, MUSEMENT shall endeavour to train the Supplier on the TUI Policies from time to time (in a format and at a frequency to be determined by MUSEMENT in its absolute discretion) in accordance with Applicable Laws.

MUSEMENT and the Supplier shall work together collaboratively to ensure ongoing compliance with the TUI Policies and Applicable Laws.

If requested by a party, the other party shall provide reasonable assistance to enable it to perform any activity required by any relevant government or agency in any relevant jurisdiction for the purpose of compliance with any of the Applicable Laws.

14. SUSTAINABLE DEVELOPMENT

The Supplier shall not do, or omit to do anything that could reasonably be expected to have an adverse effect on TUI's reputation, including in relation to its environmental, social or governance (ESG) efforts. In order to comply with this obligation, the Supplier agrees to:

Environment. i) comply with all applicable environmental laws and regulations, including but not limited to, regulations concerning waste disposal, emissions and the handling of hazardous and toxic materials, ii) minimize the environmental pollution and actively manage the Supplier's overall environmental impact by aiming to reduce energy, water and natural resource consumption and the volume of solid waste, waste water, harmful substances, and energy-related direct and indirect air emissions, iii) minimize the use of single-use plastic and promote recycling, reusing, or substitution of materials, iv) implement purchasing policies and procedures that favour sustainable and locally produced goods and services in preference to imported products, wherever possible and reasonable and v) mitigate activity that may disturb wildlife and habitats close to its business undertakings.

Social. i) comply with all applicable laws, regulations and industry standards, concerning employees, ii) protect employees by offering fair employment conditions ,including but not limited to, written contracts, correct visa and working documentation in place, working hours, documented legal minimum wage, safe working environment, vacation time, leave periods and holidays and treating employees with dignity and respect, as understood and defined by the International Labour Organisation (ILO) or applicable laws, and safeguard that they can enter or terminate their employment at their own discretion and have access to relevant information on their employee rights, iii) support diversity, inclusion and equal pay, avoid conflict zones, procure the health and safety of the Supplier's employees and provide safe working conditions and iv) promote equality and safeguard an equal treatment of employees, which includes, but is not limited to skin colour, race, ethnicity, sex, gender, religious beliefs, disabilities, political backgrounds.

Governance. i) set up a mechanism to prevent bribery and corruption and ensure not to engage in or tolerate any form of bribery and corruption, including but not limited to, giving or accepting improper

facilitation payments, ii) safeguard the independence, diversity and structure of the board as well as the appropriateness of executive pay, iii) implement measures to avoid or disclose internally conflicts of interests in its relationships and iv) avoid facilitating money laundering or funding terrorism.

15. SANCTIONS, ANTI-TRUST AND ANTI-BRIBERY

Sanctions. Each party warrants that

- neither itself nor its subsidiaries, parent company, any other affiliated company, directors, officers, member of its senior management, shareholders or other persons with controlling interests in the company (the "Associated Persons") is deemed a Sanctioned Person (defined below), is owned or controlled by or acting on behalf of any Sanctioned Person or is targeted by any trade restrictions (each the "Restricted Relationship" and collectively the "Restricted Relationships"), nor conduct business with a person or company that maintains a Restricted Relationship. Sanctioned Person shall mean any person or company with whom dealings are restricted or prohibited under the sanctions laws, regulations concerning economic or financial sanctions, export controls, trade embargoes or restrictive measures from time to time imposed, administered by the European Union, Germany, the United States and the United Kingdom, including but not limited to, (a) any person identified in any list of sanctioned persons or its respective amendments issued by EU, such as EU 2580/2001, EU 881/2002, EU 553/2007, EU 753/2011, 269/2014, 247/2022, EU 765/2006 and (b) any person, located, organized or resident in a governmental body or government instrumentality of sanctioned countries (Sanctioned Person), as far and to the extent that such adherence does not result in violating § 7 AWV (German Trade and Payments Ordinance) or EU-Reg 2271/96.
- no sanctions proceedings have been threatened or are pending against itself the Supplier or any of its Associated Person(s).
- If it is determined that Associated Persons are subject to sanctions, exceptions might apply if it is established that (a) the party itself is not subject to sanctions by the sanctioning of Associated Persons, (b) the Associated Person does not own or control the relevant party as per definition in the Applicable Law, or (c) measures have been put in place to ensure alignment with affected sanctions laws, including but not limited to, asset freezing, a restriction on voting rights and strictly refraining from making available any funds or economic benefit received under this Agreement to or for the benefit of any Sanctioned Person.

Anti-Trust. The parties further warrant that they operate in accordance with all applicable competition laws of any country in which they have assets or carry on or intend to carry on business or where their activities may have an effect, and the parties shall maintain strict controls on information exchange to ensure compliance with competition laws, and to prevent the disclosure of commercially sensitive information.

Anti-Bribery and Corruption. The parties take a zero-tolerance approach to bribery and corruption. The parties agree that they will comply with all anti-corruption and anti- money laundering legislation during the term of this Agreement. Furthermore, the parties agree that no public official has any legal or beneficial interest in any payments made under this Agreement.

Licenses. the Supplier possesses all necessary licenses in order to conduct its business.

16. AUDITING RIGHTS

The Supplier shall maintain full and accurate records, data, information and documentation in relation to the performance of its duties and compliance with its obligations under this Agreement, the TUI Policies and Applicable Laws. MUSEMENT is entitled to request such information from the Supplier to

demonstrate its compliance at any time. This includes but is not limited to requesting the Supplier to complete self-assessments, disclosing relevant policies or procedures, to inspect and take copies of all certificates, licenses, consents, permits, financial and management accounts and other documents which the Supplier is required to have by law or under the terms of this Agreement as far as inspection is lawful, in particular with regard to applicable data protection law, applicable anti-trust law, applicable anti-bribery and corruption laws and/or confidentiality obligations towards third parties.

MUSEMENT may conduct on-site audits of the Supplier itself and/or order third party audits during regular opening hours of the Supplier. Such audits may be conducted at least twice per calendar year without reason, or more frequently in the event of suspected breaches of this Agreement. Where possible, MUSEMENT will provide prior written notice. In the event of an incident or alleged breach of TUI's Policies or Applicable Laws, of severity¹, the audit may be made without prior written notice.

The Supplier must use its best endeavours to collate any relevant data and information from its subcontractors.

The Supplier should regularly review both its own operations and the operations of its supply chain partners to ensure compliance with the terms of this Agreement. MUSEMENT shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier's business.

17. VIOLATIONS, RIGHTS OF SUSPENSION AND TERMINATION

17.1 The Supplier is obliged to immediately report any suspected violations of this Agreement, the TUI Policies and the Applicable Laws. MUSEMENT may request additional information related to the breach and the Supplier should provide such information (to the extent that it is able) as soon as reasonably practicable and lawful, in particular with regard to applicable data protection law, applicable anti-trust law, applicable anti-bribery and corruption laws and/or confidentiality obligations towards third parties.

17.2 Notwithstanding any other statutory or contractual rights to terminate the Agreement MUSEMENT may terminate the Agreement at any time with immediate effect by giving written notice to the Supplier in the event of breaches by the Supplier of the TUI Policies or Applicable Laws, if the Supplier does not cure such breach within a reasonable deadline set by MUSEMENT. A deadline is dispensable if the Supplier seriously and definitively refuses to comply with this Agreement as well as in cases of gross negligent or intentional breaches.

18. FORCE MAJEURE.

18.1. Neither party shall be responsible or liable for or deemed in breach of this Agreement because of any delay or failure in the performance of this Agreement due to any event or circumstance the occurrence and the effect of which the party affected thereby is unable to prevent and avoid, including, without limitation acts of God; government regulation, curtailment of transportation facilities, strikes, lock-outs or other industrial actions or trade disputes of whatever nature (whether involving employees of a party or a third party), terrorist attacks, haze, sabotage, riots, civil disturbances, insurrections, national emergencies (whether in fact or law), blockades, acts of war (declared or not), etc. (a "Force Majeure Event"). The non-performing party shall give the other party written notice describing the particulars of the Force Majeure Event as soon as possible and the Supplier shall inform TUI on whether the Event may be postponed to a later date or cancelled or this Agreement terminated.

19. FINAL PROVISIONS

¹ As defined in the UN Guiding Principles on Business and Human Rights, Principle 14 and commentary

19.1. The Parties are autonomous entities and are not in any manner linked to each other by a permanent relationship or coordination obligation. Each of the parties expressly excludes any intention to establish a subordinate, associative, or joint venture relationship between them.

19.2. The Supplier shall not cede and/or transfer this Agreement to third parties in any manner.

19.3. This Agreement constitutes the entire agreement between the Parties with respect to the matters dealt with herein. This Agreement cancels and supersedes all previous accords between the parties in relation to the subject matter of the Agreement.

19.4. The Agreement may be amended only by written deed signed by the parties on penalty of invalidity.

19.5. No waiver of an entitlement to assert a right or non-fulfilment shall be considered valid unless it is expressly stated in writing and signed by the Party issuing the waiver.

19.6. All the communications and materials indicated at articles 1, 2 and 5 herein above shall be transmitted by the Supplier to MUSEMENT via email at the following address: partners@musement.com. Save as otherwise provided in this Agreement, any other written communication to MUSEMENT relating to the Agreement is valid and effective if made by fax or registered mail with return receipt to the following addresses: as for Musement S.p.A.: email partners@musement.com as for the Supplier: email as indicated in the relevant "Supplier" section at the <http://business.musement.com> web application^{[L]_{SEP}}. For communications: by registered mail with return receipt, the date of receipt shall be the date indicated on the advice of delivery. Communications by registered letter may be sent in advance by fax, in which case the date indicated on the fax shall prevail over the date indicated on the advice of delivery of the registered letter.

19.7. This Agreement has been the subject of comprehensive and analytical negotiations between the Parties, which have examined every individual clause and fully assessed its effects. This Agreement shall therefore be deemed to have been drawn up jointly by the Parties and no presumption may arise in the sense of favouring or prejudicing the Party that drafted any particular provision hereof.^{[L]_{SEP}}

20. APPLICABLE LAW AND VENUE

20.1. This Agreement is governed by Italian law. Any dispute in any manner related to the interpretation, validity, performance or termination of the Agreement shall be subject to the exclusive competence of the Court of Milan, notwithstanding any possible connection and/or consolidation of actions.

20.2. Without prejudice to clause 20.1 above, pursuant to Art. 1341 of Italian Civil Code the Supplier in any case expressly accepts and undersigns clauses 2.3 (refunds to third parties); 8.1 (limitations of MUSEMENT's liability); 9.3 (right to withdraw Products or Service or suspend access to the Portal); 11 (term and withdrawal); 19.2 (prohibition of transferring the agreement); 20 (applicable law and exclusive jurisdiction of the Court of Milan) of this Agreement.

21. DAC7 Obligations

21.1 The Supplier acknowledges that MUSEMENT is considered a Reporting Platform Operator subject to certain obligations deriving from COUNCIL DIRECTIVE (EU) 2021/514 of 22 March 2021, which amended Directive 2011/16/EU on administrative cooperation in the field of taxation, transposed into Italian Legislative Decree no. 32 of 2023 (jointly referred to as the "DAC7 Obligations"), as subsequently supplemented and amended. In particular and without limitation, DAC7 Obligations oblige MUSEMENT to request for, and the Supplier to provide MUSEMENT with, certain information.

21.2 Should the Supplier not provide MUSEMENT with all of the information required under DAC7 Obligations, it remains understood that after two reminders by MUSEMENT following the initial request by the same, but not prior to the expiration of 60 days, MUSEMENT shall have the right to close the account of the Supplier and to prevent the Supplier from re-registering on the Platform or, in the alternative at MUSEMENT's choice, MUSEMENT shall have the right to withhold the payment of the Supplier Consideration as long as the Supplier does not provide the information requested.

ANNEX I. TUI Information Security Schedule

Technical and organisational measures to ensure the security of data

This Schedule sets out TUI's requirements and the Supplier's information security responsibilities relating to the Services. Where relevant references to TUI include 'data exporter' and Supplier include 'data importer'.

Certification and assurance of processes and products

1. The Supplier should hold a valid SOC 2 Type II, ISO 27001, or an equivalent level of certification and/or assurance as agreed with TUI and will provide evidence of such.
2. The Supplier will conduct audits at least annually of the security of computers, computing environment and physical data centres that it uses to process TUI Data. The audit will be performed by a qualified, independent, third party security auditor at Supplier's selection and expense.
3. The audits will result in the generation of an audit report which will clearly disclose any material findings by the auditor. Audit reports shall be subject to non-disclosure and distribution limitations of Supplier and the auditor. The Supplier will:
 - a. endeavour to promptly remediate critical issues raised in the audit reports;
 - b. provide TUI with a copy of the audit reports within four (4) weeks of issue and evidence of remediation of the critical issues within four (4) weeks of the auditor agreeing any such remediation; and
 - c. provide TUI with additional information as may be required to assist its understanding of the audit reports.
4. The Supplier will, according to the actual security risk, its likelihood and impact (the "**Assessed Risk**"):
 - a. implement controls over the use of or access to TUI Data and must, upon request from TUI, provide evidence of the implementation of such measures;
 - b. include security as an appropriate consideration when deciding on the selection of hardware, software and other equipment;
 - c. include security as part of its change impact assessment;
 - d. implement practices that identify new vulnerabilities from introduced or planned changes;
 - e. implement layers of protection to provide defence in depth where reasonably practicable;
 - f. agree with TUI a means through which the security of the technology can be tested and verified by the Supplier; and
 - g. identify to TUI the security legislation, regulations and standards that are appropriate to safely conduct its business and deliver the Services.

Internal IT and IT security governance, management and accountability

5. The Supplier will:
 - a. appoint a security risk manager within its leadership team who is accountable for managing the Assessed Risk for the Services in accordance with the terms of this Schedule;

- b. define and allocate security responsibilities, accountabilities, authority and resources within the team providing the Services to TUI, to ensure that the requirements of the TUI Group Manual – IT Security are properly followed where relevant;
- c. ensure all members of its team who have access to TUI's sites, TUI's IT infrastructure and systems that support TUI's business are made aware of TUI's Security policies on their induction and no less than annually thereafter; and
- d. provide appropriate training and development so that all team members providing the Services have the competence to make an appropriate contribution to effective security according to their role.

Anonymisation, pseudonymisation and encryption of data

- 6. If the Supplier is processing or controlling Personal Data, relevant privacy-related technical control(s) will be used to help protect the information, including:
 - a. encryption (to prevent unauthorised disclosure during storage and transmission) with effective encryption key management (e.g. when handling, storing and archiving keys);
 - b. data masking (e.g. via pseudonymisation (as defined in the Data Protection Legislation), data obfuscation, data de-identification, data scrambling or data shuffling), which involves concealing parts of information (e.g. names, addresses, social security numbers and credit card numbers) when being stored or transmitted;
 - c. tokenisation, which substitutes valid information (e.g. database fields or records) with random information and provides authorised access to this information via the use of tokens;
 - d. protecting privacy-related metadata (e.g. document attributes or descriptive information that may contain Personal Data such as the name of the person who last updated a file); and
 - e. anonymising data where the services do not or no longer require the identification of a data subject.
- 7. Relevant technical control(s) will be used to help protect Confidential Information including encryption (to prevent unauthorised disclosure during storage and transmission) with effective encryption key management (e.g. when handling, storing and archiving keys).
- 8. Appropriate encryption technology should be used to safeguard (by default) all data stored on internal hard disk drives. File-based encryption software should be used to safeguard individual files and folders (including files on portable storage media and flash memory cards, such as secure digital (SD)).

Ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- 9. The Supplier will:
 - a. as far as is reasonably practicable, categorise IT systems according to the potential impact to TUI of their loss of confidentiality, integrity and availability ("**Categorisation**"); those with significant potential impact will be notified to TUI;
 - b. as far as is reasonably practicable, routinely assess if there are any actual or potential security threats to IT systems and the likelihood of those threats being realised (the "**Threat**");
 - c. identify and take steps to minimize, mitigate or manage the Assessed Risk that its people, including staff, contractors and sub-contractors, pose to TUI; and

- d. build resilience into the processes and technology used in delivery of the Services to reduce the likelihood and impact of a security incident, in accordance with the Assessed Risk.

The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident

10. The Supplier will:

- a. investigate and document security breaches, events and incidents, and report its findings without undue delay to TUI within the stated timeframe, except where otherwise agreed;
- b. routinely share with TUI any information and intelligence that it becomes aware of from outside of its enterprise that relates to the security of the IT systems and Services;
- c. determine and collect information available from diverse sources within its operations so that it can identify trends and anomalies that might indicate breaches of security in connection with the IT systems and Services under this Agreement; and
- d. identify how it prepares for, and is able to undertake command and control of, a security incident and how it determines an effective response, including how it would support TUI in its management of any incident in connection with the IT systems or Services.

Regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

11. The Supplier will:

- a. routinely assess if there are any weaknesses to IT systems that could allow an attacker to affect their security and identify how these vulnerabilities may be removed (the “**Vulnerability**”);
- b. identify vulnerabilities to IT systems and the Services and implement appropriate security controls (e.g. patching) in accordance with the Assessed Risk;
- c. apply appropriate security controls to manage the Assessed Risk; and
- d. at least quarterly, conduct risk assessments of Threat and Vulnerability for the IT systems, according to their Categorisation and consider the likelihood and potential impact of risks being realised.

12. The Assessed Risk will be documented by the Supplier and taken into account in the performance of its obligations under this Schedule, with the resulting actions also documented. This documentation will be made available to TUI on request.

Users’ identification and authorisation

13. The Supplier will maintain an approved process for authorising users, which should:

- a. be defined in writing, approved by the relevant owner and applied to all users;
- b. associate access privileges with defined users (e.g. using unique identifiers such as User IDs) to provide individual accountability;
- c. assign users with default access based on the principle of least privilege (e.g. 'none' rather than 'read');
- d. ensure redundant identifiers (e.g. User IDs) are not reissued for use; and

- e. cover authorisation of user access in exceptional circumstances (e.g. where access control mechanisms are not available, practical or safe or where technical functionality is not available).
14. A file or database containing details of all authorised users should be established and maintained by designated individuals and protected against unauthorised change and unauthorised disclosure.
 15. Details of authorised users will be reviewed on a regular basis (at least twice per year, and more frequently for users with special access privileges) to ensure that access privileges remain appropriate and ensure that redundant authorisations have been deleted (e.g. for individuals who have changed roles or left the organisation).

Protection of data during transmission and storage

16. TUI Data should be protected throughout its lifecycle (i.e. during creation, processing, storage (including backup and archiving), transmission and destruction). The technical operating measures described in paragraphs 6, 7 and 8 (as relevant) will apply to data during transmission and storage.

Physical security of locations at which data are processed

17. The Supplier will ensure that all means of physical and electronic access to assets are known, understood and controlled in accordance with their Categorisation.

Event logging

18. The Supplier will define and maintain a capability to detect, log and report to TUI that a security event or incident has occurred that may have or has had an impact on the IT systems and Services.

System configuration, including default configuration

19. Security architecture principles should be applied when developing and implementing security including:
 - a. secure by design (e.g. considering the security requirements of a business application or system as part of its overall requirements to protect itself and the information it processes and to resist attacks);
 - b. defence in depth (e.g. using multiple layers of different types of protection) to avoid reliance on one type or method of security control;
 - c. secure by default (e.g. setting preselected options to limit the level of inherent vulnerability and making only necessary services and features available);
 - d. least privilege (e.g. only granting the minimum possible access privileges to software and users);
 - e. default deny (e.g. denying access to information and systems by default to prevent unauthorised access);
 - f. fail secure (e.g. in the event of a system failure, information is not accessible to unauthorised individuals, remains available to authorised individuals and cannot be tampered with or modified);
 - g. secure in deployment (e.g. by providing complementary tools and guidance to help support system administrators and users, ensuring configuration is not difficult and software updates are simple to deploy); and
 - h. usability and manageability (e.g. security controls should not obstruct users in performing their work or be difficult to manage).

20. Hardware, software and network equipment should be:
 - a. subject to system hardening (e.g. changing default vendor passwords; changing default administration passwords; removing or disabling unnecessary accounts, services, applications, system utilities, protocols and scripts; and applying secure configuration settings); and
 - b. protected by deploying appropriate security software; encrypting sensitive information; logging important security-related events; protecting against unauthorised access; restricting access to corporate networks and providing physical security protection.
21. Specifically for Supplier's end-points that are connected to TUI's network, the end-points must:
 - a. be running a version of operating system (e.g. Microsoft Windows, Apple macOS, Linux, iOS etc.) currently in support by the operating system vendor;
 - b. have the latest updates to the operating system installed;
 - c. have Endpoint Detection and Response (EDR) software installed as agreed with TUI;
 - d. not have been altered to disable built-in security mechanisms within the operating system (e.g. 'jailbroken' (or equivalent)); and
 - e. only connect to TUI's network using an agreed connection method (e.g. VPN or similar).

Data portability and data erasure

22. Where TUI requests, or this agreement specifies, the deletion of TUI Data during or after the end of the provision of the Services such information will be undertaken using approved certified providers of secure information disposal services or other agreed methods.