SERVICE & DATA PROCESSING AGREEMENT

between

JOHNNY'S ENTERTAINMENTS (TYNESIDE) LTD

and

MERIQ AB

PARTIES

(1) Johnny's Entertainments (Tyneside) Ltd (DBA Soul Bowl), reg. no. 178015560, Pleasureland, Marine Road West, Morecambe, Lancashire, LA4 4BU (the "**Customer**").

(2) Meriq AB, reg. no. SE556627391701, Hollywoodv 73, 192 77 Sollentuna, Sweden (the "**Supplier**").

1 THE SERVICE

1.1 The Supplier is a software company providing business-to-business cloud computing services (the "**Services**"). The Services include an online software application and platform developed by the Supplier for the purposes of online booking, online scoring and web-based tournament solutions for bowling centers. The Services are further described in Appendix 1.

1.2 The Customer wishes to use the Supplier´s Service in its business operations as agreed in Appendix 1.

1.3 The Supplier has agreed to provide and the Customer has agreed to take and pay for the Supplier's Service subject to the relevant terms and conditions set forth in this Agreement (including but not limited to section 13, 15, 18-24 as regards the Services as such).

1.4 Subject to the Customer paying the agreed fee, the Supplier hereby grants to the Customer a non-exclusive, non-transferable right to use the Service in its business during the subscription term.

2 DEFINITIONS

The terms used in this Agreement, including but not limited to, "*personal data*", "*special categories of personal data*", "*process/processing*", "*controller*", "*processor*", "*data subject*", "*third country*", "*pseudonymisation*" and "*supervisory authority*", shall have the same meaning as set out and/or used in the GDPR.

Unless the context or circumstances clearly suggest otherwise, the following capitalized terms shall have the meanings stated below.

Agreement	means this document and the appendices.
GDPR	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (General Data Protection Regulation).
Instruction	means the instructions that the Customer shall provide the Supplier with in accordance with section 9 and as attached as Appendix 2.
Party/Parties	means the Customer and/or the Supplier.
Service(s)	means the services as described in section 1.1 above.

3 STRUCTURE OF THE AGREEMENT

3.1 This Agreement consists of this document and the following appendices:

3.1.1 Appendix 1 – Description and agreement regarding relevant Service

3.1.2 Appendix 2 – the Instruction (regarding processing of personal data)

3.2 If there is any inconsistency between this document and an appendix, this document shall have precedence with regard to the interpretation, if not otherwise specifically stated or if the context or circumstances do not clearly suggest otherwise.

4 PROCESSING OF PERSONAL DATA

4.1 The Supplier will process personal data on behalf of the Customer in its performance of the Service.

4.2 In this Agreement, the Customer is regarded as controller and the Supplier as processor. The Customer shall be responsible for and decide the purpose and means of the processing of personal data. The Supplier undertakes to process personal data on the Customer's behalf and solely for the purpose of enabling the fulfilment of this Agreement.

5 GENERAL REQUIREMENTS RELATING TO PROCESSING OF PERSONAL DATA

5.1 The Supplier will implement appropriate technical and organisational measures in such a way that the processing of personal data granted by this Agreement meets the requirements of the GDPR and the Supplier will ensure that the data subject's rights are protected.

5.2 The Supplier will only process personal data that are necessary for each specific purpose provided from the Customer. This obligation applies, for example, to the amount of collected personal data, the extent of their processing, the period of their storage and their accessibility. The measures taken shall further ensure that personal data - in the standard case – are not made accessible without the individual's intervention to an unlimited number of individuals.

5.3 In order to demonstrate compliance with this Agreement and the GDPR, the Supplier shall adopt internal policies and implement measures which meet in particular the principles of privacy by design and privacy by default.

5.4 Taking into account the nature of the processing, the Supplier shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

5.5 The Customer is the sole contact point in all matters regarding the Supplier's processing of personal data under this Agreement, i.e. the Customer's clients and other persons and entities are referred to the Customer in issues relating to the Supplier's processing of personal data under the Agreement.

6 THE SUPPLIER'S PERSONNEL

6.1 The Supplier shall take steps to ensure that any natural person acting under the authority of the Supplier who has access to personal data does not process them except on Instructions from the Customer, unless he or she is required to do so by Union or Member State law or this Agreement.

6.2 The Supplier also undertakes to ensure that all employees and/or consultants authorised to process the personal data, on behalf of the Customer, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7 SECURITY OF PROCESSING

7.1 The Supplier shall take all appropriate measures required pursuant to Article 32 of the GDPR. Moreover, the Supplier shall, taking into account the nature of the processing and the information available to the Supplier, assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 in the GDPR.

7.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

7.3 In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

8 NOTIFICATION OF A PERSONAL DATA BREACH

The Supplier shall, taking into account the nature of processing and the information available to the Supplier, assist the Customer in ensuring compliance with the obligations pursuant to Articles 33 and 34 in the GDPR.

9 INSTRUCTION

9.1 The Supplier will process personal data only on documented Instructions (which shall be reasonable and in written form) from the Customer, including (if applicable) with regard to transfers of personal data to a third country or an international organisation, unless required to do so by applicable Union or Member State law to which the Supplier is subject. In such a case, the Supplier shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

9.2 The Customer is entitled to update the Instruction from time to time and the Supplier shall, if possible, comply with such updated Instruction at the Customer's cost.

9.3 The Supplier shall inform the Customer if, in its opinion, an Instruction infringes this Agreement, the GDPR or other Union or a relevant Member State's data protection provisions.

10 SUB-PROCESSOR

10.1 The Supplier shall not engage another processor without prior specific or general written authorisation of the Customer. In the case of general written authorisation, the Supplier shall inform the Customer of any intended changes concerning the addition or replacement of other processors, thereby giving the Customer the opportunity to object to such changes.

10.2 If the Supplier is allowed to engage another processor for carrying out specific processing activities on behalf of the Customer, the same data protection obligations as set out in the GDPR and this Agreement or other legal act between the Customer and the Supplier shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR and this Agreement.

10.3 Where that other processor fails to fulfil its data protection obligations, the Supplier shall remain fully liable to the Customer for the performance of that other processor's obligations.

10.4 The Supplier shall comply with and respect what is stated regarding engaging sub-processors.

11 THIRD COUNTRY TRANSFER OF PERSONAL DATA

Processing and use of personal data under this Agreement shall only be carried out within the European Economic Area (as including the European Union), and more specifically storing of personal data shall be limited to that area. Any transfer to, or extension into, third countries requires prior written consent from or agreement with the Customer, which in turn will be conditional on meeting with and adhering to all and any statutory requirements, duties and preconditions of relevant EU as well as national rules, regulations and other laws regarding transfer of personal data to a third country.

12 THE CUSTOMER'S RIGHT TO INFORMATION ETC.

12.1 The Supplier shall make available to the Customer all information and documentation necessary to demonstrate compliance with the obligations laid down in Article 28 in the GDPR.

12.2 The Supplier shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor (with proven experience and procedures) mandated by the Customer. At two (2) occasions per calendar year during the term of the Agreement the Customer, or a recognised independent third party auditor appointed by the Customer, shall have the right to perform such an audit of the Supplier's processing of personal data under this Agreement in order to verify the Supplier's compliance with this Agreement and the GDPR.

12.3 The Customer shall provide a written notice at least ninety (90) days prior to the date which it intends to perform the audit in accordance with section 12.2. The audit shall be conducted during the Supplier's normal business hours and in a manner that causes minimal disturbance to the Supplier's business. Each Party shall bear its own costs in connection with an audit. By way of clarification, if the Customer engages an independent third party auditor in accordance with section 12.2, the Customer shall bear the cost for such auditor.

12.4 In case the Customer wants to perform additional audits during the calendar year, the Parties shall agree on this separately on each occasion.

13 COMPENSATION FOR THE SERVICE

13.1 The Customer shall pay compensation to the Supplier for the Service in accordance with the Supplier's pricelist.

14 COMPENSATION WITH REGARD TO DATA PRIVACY

14.1 For any additional processing that the Customer require the Supplier to perform, or any other actions or measures with regard to data privacy hereto, the Supplier is entitled to additional compensation.

14.2 The Supplier is always entitled to compensation from the Customer when performing its obligations stated in section 5.4, 8, 9.2, 12.4, 17 and 23.

15 LIABILITY AND NO LIMITATION OF LIABILITY

The Supplier shall compensate the Customer for loss incurred by the latter as result of the Supplier's processing of personal data in contravention of the Agreement. The Supplier's total liability under this Agreement shall at all time be limited to SEK 10.000 (Ten thousand SEK).

16 CO-OPERATION WITH ANY RELEVANT SUPERVISORY AUTHORITY

16.1 The Supplier shall upon request co-operate with any relevant supervisory authority in the performance of its tasks.

16.2 The Customer shall be informed when the Supplier has been contacted by relevant supervisory authorities with inquiries, orders or injunctions relating to the processing of personal data on the Customer's behalf.

17 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

The Supplier shall, taking into account the nature of processing and the information available to the Supplier, assist the Customer, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority in accordance with Article 35-36 in the GDPR.

18 CONFIDENTIALITY

18.1 The Parties hereby undertake, during the term of the Agreement and thereafter, not to disclose to any third party information regarding the Agreement, nor any other information which the Parties have learned as a result of the Agreement, whether written or oral and irrespective of form ("Confidential Information"). The Parties agree and acknowledge that the Confidential Information may be used solely for the fulfilment of the obligations under the Agreement and not for any other purpose. The receiving Party further agrees to use, and cause its directors, officers, employees, sub-contractors or other intermediaries to use, the same degree of care (but not less than reasonable care) to avoid disclosure or use of Confidential Information as it uses with respect to its own confidential and/or proprietary information.

18.2 This confidentiality undertaking does not apply to information which

a. at the date of its disclosure is in the public domain or at any time thereafter comes into the public domain (other than by breach of this Agreement); or
b. the receiving Party can evidence was in its possession or was independently developed at the time of disclosure and was not obtained, directly or indirectly, by or as a result of breach of a confidentiality obligation.

18.3 Neither shall this confidentiality undertaking apply to the extent that any Party is required to make a disclosure of information by law or pursuant to any order of court or other competent authority or tribunal or by any applicable stock exchange regulations or the regulations of any other recognised market place. In the event that any Party would be required to make any such disclosure, each Party undertakes to give the other Party immediate notice prior to any such disclosure, in order to make it possible for the other Party to seek an appropriate protective order or other remedy. Each Party also agrees and undertakes to use its best efforts to ensure that any information disclosed under this Section, to the extent possible, shall be treated confidentially by anyone receiving such information.

18.4 The provisions of this section shall remain valid for three (3) years after termination of the Agreement.

19 INTELLECTUAL PROPERTY RIGHTS

The Customer acknowledges that all intellectual property rights in relation to the Services throughout the world belong to the Supplier, that rights in the Services are licensed (not sold) to the Customer, and that the Customer has no rights in, or to, the Services or the documentation other than the right to use them in accordance with the terms of this Agreement.

20 ANNOUNCEMENTS

No party shall make, or permit any person to make, any public announcement concerning this Agreement without the prior written consent of the other Party, except as required by law, any governmental or regulatory authority (including any relevant securities exchange), any court or other authority of competent jurisdiction.

21 TRANSFER AND ASSIGNMENT

Unless otherwise agreed, a Party may not transfer the Agreement or assign any of its rights or obligations under the Agreement to any third party without the other Party's prior written consent.

22 TERM AND TERMINATION

This Agreement shall come into force upon the signing hereof by both Parties. The Parties may terminate the Agreement upon providing three (3) months written notice of termination.

23 OBLIGATION AFTER THE TERMINATION OF THE AGREEMENT

The Parties agree that on the termination of the Agreement, the Supplier shall, at the choice of the Customer, return all the personal data transferred and the copies thereof to the Customer or shall destroy all the personal data and certify to the Customer that it has done so, unless legislation imposed upon the Supplier prevents him from returning or destroying all or part of the personal data transferred.

24 AMENDMENTS

No amendments, changes, revisions, or discharges of this Agreement, in whole or in part, shall have any force or effect unless set forth in writing and signed by authorised representatives of the Parties hereto.

25 GOVERNING LAW AND DISPUTE

25.1 This Agreement shall be governed by and construed in accordance with the substantive laws of Sweden.

25.2 Any dispute, controversy or claim arising out of or in connection with this Agreement, or the breach, termination or invalidity thereof, shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (the "SCC"). The Rules for Expedited Arbitrations shall apply, unless the SCC in its discretion determines, taking into account the complexity of the case, the amount in dispute and other circumstances, that the Arbitration Rules shall apply. In the latter case, the SCC shall also decide whether the Arbitral Tribunal shall be composed of one or three arbitrators.

25.3 The seat of arbitration shall be Stockholm, Sweden.

25.4 The language to be used in the arbitral proceedings shall be Swedish.

25.5 The Parties undertake and agree that all arbitral proceedings conducted with reference to this arbitration clause will be kept strictly confidential. This confidentiality undertaking shall cover all information disclosed in the course of such arbitral proceedings, as well as any decision or award that is made or declared during the proceedings. Information covered by this confidentiality undertaking may not, in any form, be disclosed to a third party without the prior consent by the other Party.

This Agreement has been signed and executed in two (2) original copies, whereof the Parties have retained one each.

Place, date

Johnny's Entertainments (Tyneside) Ltd	Meriq AB
Authorised signatory	*Authorised signatory*
Scott Robson	Erik Fischbach
Printed name	*Printed name*

APPENDIX 1

DESCRIPTION

The following document is the Description of the Service.

Definitions used herein shall have the same meaning as in the main document of this Agreement unless the circumstances clearly state otherwise.

ONLINE RESERVATIONS

End users access the Meriq online reservation system from the customer's website. It allows end users to make reservations for bowling and other activities, such as birthday parties. If activated by the center it is also possible to pay for reservations online, where payments are handled by the chosen payment processor in an externally hosted payment window. Upon completion the reservations are flagged for download. They are then downloaded to the system used in the center, either by using a Meriq application or by direct integration in the center. Reservations are also confirmed by email which are sent by the Meriq online reservation system.

APPENDIX 2

INSTRUCTION

The following document is the Instruction.

Definitions used herein shall have the same meaning as in the main document of this Agreement unless the circumstances clearly state otherwise.

1. CONTACT DETAILS

CONTROLLER (CUSTOMER)

Company name:	Johnny's Entertainments (Tyneside) Ltd
Reg. No:	178015560
Address:	Pleasureland, Marine Road West, Morecambe, Lancashire, LA4 4BU
Telephone:	01524424212
E-mail:	scott@jetltd.co.uk
Contact person:	Scott Robson

PROCESSOR (SUPPLIER)

Company name:	Meriq AB
Reg. No:	SE556627391701
Address:	Hollywoodvägen 73, 192 77 Sollentuna, Sweden
Telephone:	+46-8132047
E-mail:	info@meriq.com
Contact person:	Erik Fischbach

2. PROCESSING OF PERSONAL DATA

CATEGORIES OF PERSONAL DATA

The following categories of personal data will be transferred between the Customer and the Supplier:

ONLINE RESERVATIONS

- Name
- Telephone number
- E-mail address
- Birth date
- Address
- Transaction details (where applicable)

SPECIAL CATEGORIES OF PERSONAL DATA AND PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

The Customer will transfer the following special categories of personal data to the Supplier:

- None

The Customer will transfer the following personal data relating to criminal convictions and offences to the Supplier:

- None

CATEGORIES OF PROCESSING

The following categories of processing are performed by the Supplier:

ONLINE RESERVATIONS

- Collection of customer details for the purpose of creating a reservation
- Storage of customer details on the online reservation servers
- Forwarding of customer details to the backend system used by the Customer
- Erasure of customer details seven days after the date of the reservation

CATEGORIES OF DATA SUBJECTS

The following categories of data subjects are processed:

- Customers (public system)
- Employees (admin system)

PURPOSE OF THE PROCESSING

The Customer's purpose of the processing is:

- Deliver the service(s) described in Appendix 1

3. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

GENERAL TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Supplier shall implement the following technical and organisational measures:

ACCESS CONTROL OF PROCESSING AREAS

The Supplier shall implement the following suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used:

1. Implement electronic access control to enter buildings hosting Personal Data.
2. Ensure that policies are in place to ensure only authorized individuals gain access to sensitive areas such as data centers, LAN rooms, phone closets and any other location where Personal Data is processed or stored. Ensure all access rights to such areas are revalidated semiannually.
3. Maintain an actively monitored alarm system that physically secures sensitive areas (includes, LAN rooms, labs, and any other area where processing of Personal Data will take place).

ACCESS CONTROL TO THE SYSTEM

In order to prevent logical access to its equipment or applications processing Personal Data by unauthorized persons, the Supplier shall take reasonable steps to implement and maintain the following measures:

1. Ensure that a unique identifier must be associated with each user of a system (network, server, database, application).
2. Ensure that the issuance of access accounts and privileges requires management approval and are reviewed every 6 months.
3. Maintain an access control list (ACL) for all systems containing Personal Data and review regularly.
4. Practice least privilege rule and the right to know principle when granting user access.
5. Ensure that processes are in place to suspend the access authorizations within 24 hours of users whose employment at Supplier ends (termination, transfer, etc.).
6. Ensure that each user's identity is verified when the user attempts to logon through the use of passwords, multi factor authentication or biometric data.
7. Set automated password protected screen-lock after more than 20 minutes of inactivity.
8. User passwords must have the minimum length of 8 characters, containing at least one character from 3 out of 4 categories (upper case letter, lower case letter, number and special character).
9. Administrator, system level and service account passwords must have a minimum length of 15 characters, containing at least one character from 4 out of 4 categories (upper case letter, lower case letter, number and special character).
10. All installation and vendor-default passwords provided with new hardware, system software and applications must be reset upon installation.
11. Standardize servers and operating system builds and configuration in accordance with industry standards so as to be resistant to attacks.
12. Maintain a documented patch management process and perform updates on systems with Critical and High Risk vulnerabilities within 2 weeks from the patch release and all others within one month.

ACCESS CONTROL TO PERSONAL DATA

The Supplier shall take reasonable steps to prevent logical access to Personal Data by unauthorized persons by implementing and maintaining suitable measures to prevent unauthorized reading, copying, alteration or removal of the media containing Personal Data, unauthorized input into memory, reading, alteration or deletion of the stored Personal Data. This will be accomplished by the following measures:

1. Maintain a written data classification and handling policy and an inventory of records with classification with physical and electronic location provided.
2. Supplier shall ensure that Personal Data is encrypted in transit using non deprecated industry standard protocols (e.g. SSH/SCP/SFTPV2, TLSv1.2 or greater).
3. Supplier shall ensure an industry standard level of encryption of Personal Data appropriate to the risks that are presented by the processing of Personal Data at rest. Notwithstanding, all backups of Personal Data shall be encrypted on backup media.
4. Personal Data may only be downloaded to a Supplier's PC, laptop, mobile device, or removable storage if hard disk encryption is enabled on that device.

TRANSMISSION CONTROL

The Supplier shall implement the following measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media:

1. Ensure perimeter networks are physically or logically separated from internal networks containing Personal Data.
2. Setup firewalls between: Internet and web facing systems; web facing systems and application systems; application systems and internal networks.
3. Firewall rules shall be reviewed annually.
4. Restrict and control wireless network access using industry standard wireless security protocols, but nothing less secure than WPA2.
5. Restrict and control remote network access and require the use of VPN.

INPUT CONTROL

The Supplier shall take reasonable steps to ensure the ability to check and establish whether, and by whom, Personal Data was inputted, modified or removed from the data processing equipment as follows:

1. Monitor to detect and generate alerts for unauthorized changes.
2. Ensure that emergency changes require appropriate level management approval before implementation.
3. Ensure that consequences for policy violations are established, communicated, and acted upon.

ORGANIZATION CONTROL

The Supplier shall take reasonable steps to arrange the internal organization in such a way that it meets the specific requirements of data protection and implement and maintain the following measures:

1. Maintain a written information security policy that is approved annually by Supplier management team and published and communicated to all Supplier employees and relevant third parties.
2. Maintain a dedicated security and compliance function to design, maintain and operate security in support of its "trust platform" in line with industry standards. This function shall focus on system integrity, risk acceptance, risk analysis and assessment, risk evaluation, risk management and treatment statements of applicability and vendor management.
3. Maintain data protection, security awareness and compliance program, procedures and tools which address information security threats and best practices; as well as information security policies, procedures, and controls in place to protect Personal Data.

AVAILABILITY CONTROL

The Supplier shall implement the following measures to ensure that personal data are protected from accidental destruction or loss:

1. Manage a security incident response process.
2. Maintain contingency planning policies, procedures, and tools which define roles and responsibilities and provide clear guidance and training on the proper handling of contingency events including: natural threat events such as floods, tornadoes, earthquakes, hurricanes, and ice storms; accidental threat events such as chemical spills, and mechanical or electrical failures; and intentional acts such as privacy and security breaches, bomb threats, assaults, and theft.
3. Have a business continuity/disaster recovery plan in place for the restoration of critical processes and operations of the Supplier's services at the location(s) from which the Supplier's services is provided. Supplier shall also have an annually tested plan in place to assist in reacting to a disaster in a planned and tested manner.
4. Perform full backups of the database(s) containing Personal Data in a secure manner to ensure availability in line with the criticality of the data.

ASSET CONTROL

In order to ensure the protection of equipment or applications processing Personal Data, the Supplier shall take reasonable steps to implement and maintain the following measures:

1. Ensure that procedures and tools are in place to identify and track all equipment and media used in the processing Personal Data.
2. Assign responsibility for all equipment and media to one or more custodians.
3. Perform annual full review of the asset inventory and signoff of the asset inventory for accuracy and to identify missing equipment and media.

APPLICATION CONTROL

In order to ensure the protection of equipment or applications processing Personal Data, the Supplier shall take reasonable steps to implement and maintain the following measures:

1. If applicable, prior to application release, conduct penetration tests, web application vulnerability tests and high severity vulnerabilities mitigation.
2. Ensure that developers are trained on industry-standard secure developing best practices.
3. Application security vulnerabilities that affect Personal Data shall be corrected within a reasonable time after identification.

CHANGE AND SEPARATION OF DATA CONTROL

The Supplier shall take reasonable steps to implement and maintain the following change control measures for processing of Personal Data:

1. Maintain change management processes that include documentation of the purpose, security impact analysis, testing plan and results, and appropriate management authorization for all changes on systems processing Personal Data.
2. The configuration of systems processing Personal Data must be validated prior to release in the production network.
3. Maintain physically and / or logically separate development/ testing/ staging environments from production environments where Personal Data is processed.

STORAGE LIMITATION

The Supplier will process and store personal data for the following time periods:

Online reservations: Personal details are pseudonymised in the online reservation system seven days after the date of the reservation.

4. SUB-PROCESSOR – SPECIFIC AUTHORISATION BY THE CUSTOMER

The Customer approves the following sub-processors to carry out processing activities on behalf of the Customer: **Amazon Web Services**

Where does the processing take place (geographical location)? **European Union**