A. Terms & Conditions

1. Definitions

1.1. “**Agreement**” means this Order Form, applicable SOW’s, applicable NDA’s, the provisions in any documents or online resources referenced in other parts of this Agreement and any other Exhibits and/or Schedules to which in this Agreement reference is made;

1.2. **“Customer Data”** means any and all data that relates to an identified or identifiable individual who is a customer or prospective customer of the Customer (and such term shall include, where required by Applicable Data Protection Laws, unique browser or device identifiers), which is acquired or collected by a Party or its representatives during the performance of this Agreement;

1.3. “**Deliverables**” means Software and encoder(s) if included on an Order Form;

1.4. “**Intellectual Property Rights**” or “**IPR**” means any and all intellectual property rights (whether registered or unregistered) and all applications of the same, anywhere in the world, including without limitation all of the following and all rights in, arising out of, or associated therewith: (i) procedures, designs, inventions, discoveries, and all patents issued or issuable thereon, (ii) works of authorship, copyrights and other rights in works of authorship, trademarks, trade secrets, know-how and database rights;

1.5. “**Party**” or “**Parties**” means each of Livery and Customer, individually, or both of them, collectively, as the context requires, in this Agreement;

1.6. “**Services**” means the non-exclusive information technology-related consulting, training, development, implementation, advice or customization services relating to the Software to be provided by Livery to the Customer as detailed and as specified in the applicable Order Form including the provision of access to the Software under the terms of this Agreement;

1.7. “**Software**” means the Livery software and/or software exploited by Livery and its associated documentation, reporting tools, future updates and enhancements and any specific development delivered by Livery under this Agreement at Customer’s request;

1.8. “**Term**” means the term of this Agreement, being either the Initial Term or any Renewal Term or extension thereof in accordance with this Agreement;

1.9. “**Third-Party Services**” means third-Party Web-based, data, mobile, offline or other service or software application functionality that is provided by a third Party and that interoperates with the Software.

2. Services

Livery will provide the Services (including the Software) to Customer pursuant to the terms of this agreement with effect from the Effective Date and for the duration of this Agreement.

3. Third Party service providers

3.1. **Third-Party Services and Separate Terms**. Livery may make available third-Party products or services. Any acquisition by Customer of such products or services, and any exchange of data between Customer and any non-Livery provider, product or service is solely between Customer and the applicable non-Livery provider and the third-Party provider’s terms and conditions apply between Customer and the relevant third Party in connection with those products and/or services. Such third-Party’s terms and conditions are in addition to the terms of this Agreement. Customer must accept the third-Party provider’s terms to receive their products and services. Livery is not liable for any third-Party product or service except where expressly agreed by Livery in writing and clearly stated.

3.2. **Third-Party Services and Customer Data and Systems**. If Customer chooses to use a Third-Party Service with Livery Software and/or Services, Customer grants Livery permission to allow the Third-Party Service and its provider(s), if any, to access Customer Data and Customer’s systems as required for the interoperation of that Third-Party Service with the Software and/or Services. Livery is not responsible or liable for any disclosure, modification or deletion of Customer Data and Customer’s systems resulting from access by such Third-Party Service or its provider. Customer warrants that it has permission to grant this permission to Livery.

3.3. **Integration with Customer Data and Systems, and Third-Party Services**. The Software may contain features designed to interoperate with Customer Data and Systems and with Third-Party Services. To use features that interoperate with Third-Party Services, Customer may be required to obtain access to such Third-Party Services from their providers, and may be required to grant Livery access to Customer account(s) for such Third-Party Services. Livery cannot guarantee the continued availability of Software features that interoperate with Customer Data and Systems and with Third-Party Services, and may cease providing them without entitling Customer to any refund, credit, or other compensation, if for example and without limitation, the provider of Customer Data and Systems or Third-Party Services ceases to make Customer Data and Systems or Third-Party Services available for interoperation with the corresponding Software features in a manner acceptable to Livery. Livery does not warrant or support Customer Data and Systems, Third-Party Services or other non-Livery products or services, whether or not they are designated by Livery as “certified” or otherwise, unless expressly provided otherwise in the Order Form.

4. Term of the Agreement & Termination

4.1. Unless previously terminated by either Party in accordance with the termination provisions set out below, this Agreement shall commence on the Effective Date and continue in full force and effect until the last end of the Initial Term. Following the Initial Term, this Agreement shall automatically renew for successive periods with a duration as defined under Renewal Term (each, a “Renewal Term”, and together with the Initial Term, the “Term”).

4.2. This Agreement may be terminated at the end of the Initial Term or any Renewal Term by either Party by providing written notice of non-renewal to the other Party at least 30 days prior to the end of the Initial Term or any Renewal Term.

4.3. The Customer shall return any rental hardware, if applicable, within 15 days after the termination of the Agreement. Livery shall invoice Customer an amount equal to €2,500 if the rented hardware is not timely returned or if the hardware is damaged.

4.4. In addition, without prejudice to any rights and remedies that may have accrued under this Agreement, either Party may terminate this Agreement immediately upon written notice to the other Party if the other Party:

(i) commits a material breach of this Agreement and fails to cure such breach of this Agreement within 30 days of receiving notice of the breach;

(ii) becomes insolvent, or admits in writing to being insolvent or is unable to pay its debts as they become due;

(iii) has appointed a receiver, liquidating officer or trustee for all or substantially all of its assets; or

(iv) files for bankruptcy

5. Fees and Payment

5.1. The prices of the Software licenses and Services ordered by Customer under this Agreement are set out in the Order Form. Unless agreed otherwise, these prices are quoted in Euro and exclude VAT, taxes and other costs (transport, packing, insurance, import and export duties, etc).

5.2. Unless otherwise provided in Section A of this Order Form, Livery shall invoice Customer on a monthly basis via email for any Services and Software licenses provided under this Agreement, and such invoices shall be expressed in Euro.

5.3. Customer shall make payment of each such invoice by the due date stated in that invoice or within 15 days of receipt of the invoice as based on the email timestamp, whichever is later.

6. Hosting

The hosting of the Software may include: (a) the supervision of the server; (b) the allocation, as appropriate, of agreed Concurrent User capacity on a server supervised by Livery; (c) the supervision of the correct operation of the infrastructure required for the hosting; (d) the supervision of access to the Software. If applicable, hosting offered by Livery is defined in the appropriate Order Form.

The physical hosting will be done by third-Party hosting providers such as Akamai and Amazon AWS. For terms of physical security, access to the Software, the Customer data and firewalls the standard terms and conditions from Akamai and other hosting providers apply.

7. Maintenance of the Software

Maintenance operations are essential for the proper operation of the Software. Livery provides its Customers with Encoder and SDK’s updates as it deems necessary. Maintenance operations will be scheduled and agreed upon by the Parties. Customer will cooperate with Livery and provide access and any other assistance Livery needs to update its software.

During the term of this Agreement, Livery shall provide technical assistance in the form of a technical support contact and remote diagnostics assistance to Customer with respect to the use and maintenance of the Deliverables in accordance with this Agreement. Customer will provide, at Livery’s request, access to relevant systems and data needed for Livery’s technical assistance.

8. Warranty

Livery warrants Customer that:

8.1. The Services will be performed in accordance with proper established industry standards and in accordance with the provisions of this Agreement.

8.2. It has the right to license the Software to Customer.

8.3. It is understood between the Parties that Livery does not warrant that the Software is 100% free from any bug at time of delivery to Customer. Livery will fix such bugs within a reasonable time frame.

8.4. No warranty can be given on performance of the “Last Mile” and end-users’ Internet Service Providers (ISPs). Examples include end user hard- and software such as devices and operating systems, all connections from the end user to the ISP as well as the ISP’s capacity itself.

8.5. When the optional on premise Livery Encoder is acquired, it is warranted against defects in materials and workmanship for a period of 1 year from the Order Effective Date ("Warranty Period"). This warranty does not cover damage resulting from accident, misuse or abuse, lack of reasonable care, the affixing of any attachment not provided with the product or loss of parts or subjecting the product to any but the specified voltage. Customer shall contact Livery account manager if the Encoder appears to be inoperable. Livery will then take the necessary steps to determine if a replacement is necessary. When replacement is needed Livery does its best effort to ship a new Encoder within 3-7 days varies depending on the destination and shipping provider.

Except as expressly provided in this Section 9, Livery provides no warranties, express, implied, statutory, or otherwise, and specifically disclaim any warranty of merchantability or fitness for a particular purpose, uninterrupted or error-free operation, or accuracy, completeness or currentness with respect to the Software and/or documentation provided by Livery, or information contained therein. Livery shall not be liable for any loss or damages arising from its acts or omissions in procuring, compiling, collecting, interpreting or reporting information contained in the Software, resource material or user documentation.

9. Intellectual Property Rights, License and Use

9.1. **Ownership**. Subject only to the rights and licenses expressly granted to Customer in this Agreement, Livery or its licensors shall retain all of their Intellectual Property Rights in the Software, the Services and their derivative works. Customer shall own all rights, including all Intellectual Property Rights, in and to, the Customer Data.

9.2. **License**. Subject to the terms of this Agreement, including any specifications and limitations set forth in the applicable Order Form, and Customer's payment obligations, during the Term of this Agreement, Livery hereby grants Customer a limited, non-exclusive, non-transferable license (without right to sublicense), (i) to access and use the Software; (ii) to access and use the Services; (iii) to access and use one or more encoders, including the software contained therein; (iv) to use Livery's application programming interfaces ("**API's**") to access reporting on the Customer Data. Livery retains all rights in the Services, Software and API's not expressly granted to Customer in this Agreement.

9.3. **Restrictions of Use**. Unless otherwise authorized in Section A this Agreement, Customer may not (and will not allow any third-Party to): (i) sell, rent, lease, license, sublicense, distribute, pledge, assign or otherwise transfer in whole or in part the Software or any interest in it to another Party; (ii) install or use the Software in a manner that circumvents or interferes with the operation of the technological measure that controls the access to the Software (iii) modify, translate, adapt or create derivative works based on the Software; (iv) remove or modify any Software markings or any notice of Livery's and/or its licensors proprietary rights; (v) use the Software to develop, test, host, or run and operate applications on behalf of third-Parties to this Agreement, without Livery's prior written consent; (vi) use the Software in any way that is contrary to the terms and conditions of this Agreement; or (vii) use the Software for any unlawful purposes. Except to the extent expressly permitted by this Agreement or applicable law, and to the extent that Livery is not permitted by that applicable law to exclude or limit the following rights, Customer may not (and may not ask or order to) decompile, disassemble, reverse engineer, or otherwise attempt to derive source code from the Software, in whole or in part.

9.4. **Manner of use**. Subject to the terms of this Agreement, including the specifications and limitations set forth in the applicable Order Form, Customer agrees not to use or permit use of the Software to display, store, process or transmit any content, that may (i) menace or harass any person or cause damage or injury to any person or property, (ii) involve the publication of any material that is false, defamatory, harassing or obscene, (iii) violate privacy rights or promote bigotry, racism, hatred or harm, (iv) constitute an infringement of intellectual property or other proprietary rights, or (v) otherwise violate applicable laws, ordinances or regulations. If Livery receives information that Customer is in violation of any of the foregoing restrictions, Livery will notify Customer, and Customer will promptly take appropriate action to resolve such violation. If Customer does not take required action in accordance with the above, Livery reserves the right, but has no obligation, to take remedial action if any material violates the foregoing restrictions, including the removal or disablement of access to such material. Livery shall have no liability to Customer in the event that Livery takes such action

9.5. **Acceptable Use Policy - General Conduct** As part of the Services Livery resells Akamai's Services and distributes Livery's Services using Akamai's Network and/or Amazon AWS. In addition to the Terms for the Manner of use in Clause 9.4, Customer confirms it will only use Livery for the lawful purposes as defined by Akamai and Amazon AWS in their respective Acceptable Use Policy, accessible at https://www.akamai.com/legal/acceptable-use-policy and https://aws.amazon.com/aup/.

Akamai's AUP addresses the following topics:

Responsibility for Content
Inappropriate and Illegal Content

Intellectual Property
Fraudulent/Misleading Content
Email and Spam
Security Violations
Akamai Rights & Remedies

10. Publicity & Communications

Livery will have the right to mention, e.g. on its website, that Customer is a Customer of Livery including generic information on how Customer uses the Software, and vice versa Customer can mention it's a Customer of Livery and how it uses the Software.

Customer approves that the email addresses of its employees or representatives Livery is communicating with can be added by Livery to Livery's mailing list and/or Slack channel for customer update and/or marketing purposes.

11. Limitation of Liability

11.1. **Limitation of Liability** In no event shall Livery or Customer's total liability arising out of this agreement exceed fifty percent (50%) of the total amount received by Livery from Customer hereunder for the Services and/or Software giving rise to the liability in the twelve months preceding the first incident out of which the liability arose. The foregoing limitation will apply whether an action is in contract, tort (including negligence), breach of statutory duty, restitution or otherwise and regardless of the theory of liability, but will not limit the Customer's payment obligations as set out in the applicable Order Form.

11.2. **Exclusion of Consequential and Related Damages**. In no event will either Party have any liability arising out of or related to this Agreement for any indirect, special, incidental, or consequential damages including, without limitation, lost profits, data, expected savings, lost revenues, goodwill (in each case whether direct or indirect), nor for any other indirect, special or incidental, consequential loss, costs or damages, whether an action is in contract, tort (including negligence), breach of statutory duty, restitution or otherwise, and regardless of the theory of liability, even if a Party have been advised of the possibility of such damages and if a Party's remedy otherwise fails of its essential purpose.

11.3. **No Limitation in Certain Cases**. Nothing in this Agreement excludes or limits a Party's liability for (a) death or personal injury caused by that Party's negligence,

(b) fraud or fraudulent misrepresentation or (c) any other liability which may not be properly limited or excluded by applicable law.

11.4. **Exclusions**. Customer assumes sole responsibility for results obtained from the use of the Services and Software and for conclusions drawn from such use. Livery shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to Livery by Customer in connection with the Services and/or Software or any actions taken by Livery at Customer’s direction.

12. Confidentiality

12.1. **Definition of Confidential Information**. “**Confidential Information**” means all information disclosed by a Party (“**Disclosing Party**”) to the other Party (“**Receiving Party**”), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third Party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party without use of or access to the Disclosing Party’s Confidential Information. The Receiving Party will protect and safeguard the Disclosing Party’s Confidential Information with the same degree of care that it uses to protect the confidentiality of its own Confidential Information of like kind (but not less than reasonable care). In addition, each Receiving Party agrees (i) not to use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement and (ii) except as otherwise authorized by the Disclosing Party in writing, to limit access to Confidential Information of the Disclosing Party to those of its employees and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements or are otherwise bound by confidentiality duties or obligations to the Receiving Party containing protections not materially less protective of the Confidential Information than those contained herein. Each Receiving Party shall promptly notify the Disclosing Party of any actual or suspected misuse or unauthorized disclosure of the other Disclosing Party's Confidential Information.

12.2. **Compelled Disclosure**. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a Party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to that Confidential Information.

12.3. **Software performance monitoring**. Customer acknowledges and accepts that Livery can use the data moving through the Software and/or systems connected with the Software, including Customer's data, to monitor performance of the Software and connected systems and proactively identify and solve issues, and to generate and use aggregated service statistics without personal data.

12.4. **Return of Confidential Information**. Upon expiration or termination of this Agreement, each Receiving Party shall return all Confidential Information received from the Disclosing Party and shall delete or destroy all confidential information of the Disclosing Party held in an electronic form and confirm such deletion or destruction to the Disclosing Party in writing.

12.5. **Confidentiality of Agreement**. Each Party shall be entitled to disclose the existence of this Agreement, but agrees that the terms and conditions of this Agreement shall be treated as Confidential Information and shall not be disclosed to any third Party; provided, however, that each Party may disclose the terms and conditions of this Agreement:

(i) as required by any court or other governmental body;
(ii) as otherwise required by law;
(iii) to legal counsel of the Parties;
(iv) in confidence, to accountants, banks, and financing sources and their advisors;
(v) in connection with the enforcement of this Agreement or rights under this Agreement; or
(vi) in confidence, in connection with an actual or proposed merger, acquisition, or similar transaction.

13. General

13.1. **Governing Law and Dispute Resolution**. This Agreement shall be governed by and construed in accordance with the laws of The Netherlands, with the exclusion of its conflict of laws rules. All disputes arising in connection with this Agreement or further contracts resulting from it will be finally settled in accordance with the Arbitration Rules of the Netherlands Arbitration Institute (Nederlands Arbitrage Instituut) whereby the place of arbitration will be The Hague, the Netherlands and the arbitral procedure shall be conducted in the English language, in writing, with one arbitrator and with the arbitral tribunal deciding in accordance with the rules of law. Notwithstanding this clause, Parties may bring proceedings in the courts of any state or territory which has jurisdiction for reasons other than the Parties' choice for the purpose of seeking an interim injunction, order or other non-monetary relief to protect Parties intellectual property rights and/or rights in Confidential Information.

13.2. **Assignment**. Neither Party will have the right to assign, transfer, or otherwise dispose of its rights and obligations under this Agreement or any Order to any third Party without the prior written consent of the other Party; *except that* a Party may assign the Agreement without such consent to its successor in interest by way of merger, acquisition, or sale of all or substantially all of its assets.

13.3. **Severability**. If any provision of this Agreement or related Schedules and Orders is held or deemed to be invalid or unenforceable in any jurisdiction or shall be changed following a decision by a national or international authority, the Parties shall endeavor to amend the provision so affected so as to make them valid and enforceable whilst reflecting as closely as possible the commercial purpose and intent of said provision. It is agreed that this invalidity or unenforceability of such provision shall not affect the other provisions of the Agreement.

13.4. **Force Majeure**. Notwithstanding anything else in this Agreement, and except for the obligation to pay money, no default, delay or failure to perform on the part of either Party shall be considered a breach of this Agreement if such default, delay or failure to perform is shown to be due to causes beyond the reasonable control of the Party charged with a default; provided, that for the duration of such force majeure the Party charged with such default must continue to use all reasonable efforts to overcome such force majeure.

13.5. **Parties terms and conditions do not apply**. This Agreement excludes any (general) terms and conditions of Parties, regardless of any (previous) reference by a Party to its own or other terms and conditions. Livery explicitly rejects any general terms and conditions declared applicable by the Customer and will never be deemed to have accepted such general terms and conditions. Any derogation from this Agreement has to be explicitly agreed on between Parties in writing.

B. Service Level Agreement (SLA)

1. Purpose

This Service Level Agreement ("SLA") Section C sets forth the parties' agreement with respect to the Services that Livery will provide to Customer under the Order Form. This SLA is an Exhibit to the Order Form and is intended to set forth the basic level of service required in order to support the delivery of the Services.

2. Service Reliability

Livery shall provide service uptime of 99,5% for the Services, where:

Availability =

([# of Minutes in Month] - [# of Minutes Planned Downtime in Month]-[# of Minutes Unscheduled Downtime])

Divided by:

([# of Minutes in Month] - [# of Minutes Planned Downtime in Month])

If Availability for the Services is less than 99,5% for a given month of the Term, Livery shall issue Customer at Customer's request a User Hour Service Credit in accordance with the schedule below, based on the total User Hours used in the calendar month of the affected Services.

Availability	User Hour Service Credit (Percentage of Availability for the month during which the Uptime commitment was not met)
More than 99,5%	0%
More than 95% and less than 99,5%	5%
More than 85% and less than 95%	25%
Less than 85%	75%

Example: if in a given calendar month the Uptime was 99% and Customer used a total of 10.000 User Hours and requested a User Hour Credit, that credit would be 500 User Hours (5% of 10.000 user hours).

To receive a User Hour Service Credit, Customer shall submit a request to Livery, with the description “Request for Service Credit” in the subject line of the email. Each request must include the following information: (a) the applicable company’s (“Customer”) name; (b) Customer’s contact name, email and telephone information; (c) date and beginning and end time(s) of outage(s); and (d) a description of the characteristics issue. Livery will review the Request and if it acknowledges it, the User Hour Service Credit will be added to the User Hour Credit for the Customer.

Unscheduled Downtime is defined as an Incident where the primary functionalities of the Services are unavailable to at least 20% of the end users as well as lasting at least 5 minutes. Unscheduled Downtime does not cover any issues arising from reasons under Exclusions and are excluded from this calculation.

Livery will make commercially reasonable efforts to ensure that the Services are free from material defects, and are available, 24 hours a day, 7 days a week.

Customer acknowledges that Livery’s Services are offered on a shared infrastructure and that other Customers’ usage may impact the performance of all Customers using that shared infrastructure. For the Data & Interactions Services of Livery, performance of the shared infrastructure primarily depends on the number of users connected at the same time, the number of users registering and/or logging in and the number of users actively using interactions, chat and other Livery features. If performance is degraded but Services are still operational, this is not considered to be an Incident.

3. Maintenance

Service Provider may modify the Service Provider System from time to time to install bug fixes and required updates (as deemed appropriate by Livery).

Livery will ensure that any planned maintenance and update events within the control of Livery will be executed in a professional manner.

Any Scheduled Maintenance in excess of 24 hours per month shall constitute unavailability for the purposes of measuring uptime against the SLA.

Livery primarily uses Mondays between 8.00 and 9.00 UTC as a recurring window for Scheduled Maintenance and is not required to send out prior notice about any maintenance done during this window. Any Scheduled Maintenance outside of this window will be announced via its Customer email list at least 24 hours in advance.

4. Monitoring & Reporting

Livery uses a system that measures the availability of Services, which it uses to detect and analyze Incidents, based on which the Availability uptime can be calculated.

5. Exclusions

This SLA applies to Services specified in the Order Form only. The following reasons, issues and/or causes are not considered to be Unscheduled Downtime as covered by this SLA and are excluded from any Availability calculations:

1. “Last Mile” and end-users’ Internet Service Providers (ISPs). Examples include end user hard- and software such as devices and operating systems, all connections from the end user to the ISP as well as the ISP’s capacity itself.
2. An issue caused by a general disruption or outage by one or more infrastructure or hosting providers that are not under control of Livery. Examples of such infrastructure or hosting providers include but are not limited to cloud services providers (for instance Amazon AWS), video CDN (for instance Akamai), SMS (for instance Twilio), DNS and/or authentication providers such as facebook, Google or OTP providers.
3. Customer integrations and APIs that are integrated with Livery, e.g. for user registration or login
4. Any use of the Services outside of the scope described in the Agreement
5. Any Force Majeure event
6. Any non-production system, such as development or staging environments
7. Slower performance of Data & Interactions caused by a large number of connected end users and/or many end users logging in and/or registering within a short timeframe.
8. Any systems or services that Customer and/or third parties have access to on a level that exceeds regular user level (e.g. root or administrator level)

6. Contacts

Unless confirmed in writing by Livery, contacts for communication on any of the topics covered by this SLA will be the Livery Contact and Customer Contact as described in Order Form Section A.

E-mail will be the primary channel for communication for any SLA related issues. At Livery’s sole discretion, additional communication methods, e.g. a dedicated Slack channel or phone, may be offered to Customer.

C. Data Protection Authority (DPA)

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") between

____
____
____

(the “Company”)

and

Livery Video B.V., a dutch company based in Amsterdam, (1033 PG) NDSM-Plein 7, registered at the chamber of commerce with number 80342418, represented by Jeroen Elfferich (CEO) (the “Data Processor”)

(together as the “Parties”)

WHEREAS

A. The Company acts as a Data Controller.

B. The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

C. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with 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).

D. The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "Contracted Processor" means a Subprocessor;

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "EEA" means the European Economic Area;

1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.8 "Data Transfer" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "Services" means the interactive video services the Company provides.

1.1.10 "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company’s documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 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, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any
Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the

Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of The Netherlands.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Amsterdam (The Netherlands), subject to possible appeal to the high court of Amsterdam (The Netherlands).

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Livery Video B.V.	**<Company>**
Signature:_____________________	Signature: ___________________
Name:Jeroen Elfferich	Name:_______________________
Title: CEO	Title:________________________
Date Signed:______________________	Date Signed:__________________

APPENDIX 1: Technical and Organizational Measures

1. Access Control to Premises and Facilities
Unauthorized access to premises and facilities is prevented through the following measures:

- Access control system: Keys and Security code for main building entrance.
- Office entrance control: Managed during office hours and locked outside office hours.
- Surveillance facilities: Video cameras at the building entrance and office spaces.

2. Access Control to Systems and Data
Unauthorized access to IT systems is prevented through both technical and organizational measures:

- Password procedures: Enforced use of strong passwords with special characters, minimum length, and regular changes; two-factor authentication where possible.
- Differentiated access rights: Based on profiles, roles (RBAC), and objects.
- Access logs: Logs are maintained for the majority of the Livery systems.

3. Disclosure Control
Control over the disclosure of personal data includes:

- Encrypted delivery: All data delivered over encrypted HTTPS.
- Protected access: Data access protected by password or secure token.

4. Job Control
Commissioned data processing is conducted according to instructions, ensuring segregation of responsibilities between the controller and processor:

- Formal commissioning: Through enterprise agreements or self-sign-up including online Terms of Service.
- SLA monitoring: Regular monitoring of Service Level Agreements.

5. Availability Control
Measures to protect data against accidental destruction or loss include:

- Backup procedures: Daily backups.
- Redundant cloud storage: Data stored in highly redundant third-party cloud services.
- Firewall policies: IP restriction on key components
- Disaster recovery plan: Established and maintained.

6. Segregation Control

Data collected for different purposes is processed separately to ensure its integrity and confidentiality:

- Microservices architecture: Functions run and administered separately.

7. Security Documentation
Maintaining security documentation ensures proper tracking and handling of security incidents:

- Security document: Comprehensive documentation of security measures.
- Incident log: Detailed logging of security incidents including incident description, date and time, and actions taken.

8. Audits
Data exporters (customer) have the right to audit data importers (Livery Video) to ensure compliance with security obligations:

- 3rd party Audit: Provided upon written request to verify compliance.

9. Assistance with Data Subject Rights Requests
Handling of Data Subject Rights Requests:

- Contact information: Requests sent to info@liveryvideo.com

10. Pseudonymisation
Personal data processing includes pseudonymization to protect individual privacy:

- Viewership data: Pseudonymized by truncating IP addresses before sending to the United States.

11. Personnel Security Management
Measures to ensure personnel security include:

- Confidentiality agreements: Employment and confidentiality agreements in place.
- Defined roles: Clear definition of roles and responsibilities.
- Training: Regular security and privacy training.
- Onboarding/offboarding procedures: Defined procedures for personnel changes.

12. Other Technical and Organizational Security Measures
Additional security measures include:

- Logging, monitoring, and alerting of the platform.
- Encryption and key management practices for data protection.
- Secure development processes, including secure coding, application testing, and controlled CI/CD procedures.
- Business continuity and disaster recovery policies and procedures in place.
- Incident response policies and procedures.
- Password management tool

These measures collectively ensure the security, integrity, and confidentiality of data processed under the Livery Video DPA

APPENDIX 2: List of Sub-processors

The following list contains an overview of the sub-processors which are utilized by the Livery Platform.

	Name of sub-processor	Livery Product	Country of Operation and Data processing	Subject matter and nature of the processing
1	AWS	Interactive & Video	Seattle, USA Frankfurt, DE	Hosting
2	Akamai	Video	Cambridge, USA	Content delivery (video)
3	Sentry	Interactive & Video	Iowa, USA	Diagnostics
4	Grafana	Interactive & Video	New York, USA	Diagnostics
5				
6				
7				

All sub-processors may have access to the Customer Personal Data for the term of the Livery Video Privacy Terms or until the service contract with the respective sub-processor is terminated or the access by the sub-processor has been excluded as agreed between Livery Video and Customer.

APPENDIX 3: Supplementary Measures for International Data Transfers

Livery Video commits to implementing the following supplementary measures based on guidance provided by EU supervisory authorities in order to enhance the protection for Customer Personal Data in relation to the processing in a third country.

1. Additional Technical Measures

1.1 Encryption

1.1.1 The personal data is ***transmitted*** (between the Parties and by Processor between data centers as well as to a sub-processor and back) using strong encryption.

- It is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of this third country.
- The parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure.
- Specific protective and state-of-the-art measures are used against active and passive attacks on the sending and receiving systems providing transport encryption, including tests for software vulnerabilities and possible backdoors.
- In cases where transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal data is also encrypted end-to-end on the application layer using state-of-the-art encryption methods.
- The encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities when data is transiting to this third country, taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them.
- The strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved.
- The encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities, the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification.
- The keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked), by Customer or by an entity trusted by Customer under a jurisdiction offering an essentially equivalent level of protection.

1.1.2 The personal data at ***rest*** is stored by Processor using strong encryption.

The encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country, taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them. The strength of the encryption and key length takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved. The encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities, the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification. The keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked).

2. Additional Organizational Measures

2.1 Internal policies for governance of transfers especially with groups of enterprises

2.1.1 Adoption of adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of formal or informal requests from public authorities to access the data.

- Especially in case of transfers among groups of enterprises, these policies may include, among others, the appointment of a specific team, composed of experts on IT, data protection and privacy laws, to deal with requests that involve personal data transferred from the EEA.
- Notification to the senior legal and corporate management and to Customer upon receipt of such requests.
- Procedural steps to challenge disproportionate or unlawful requests and the provision of transparent information to data subjects.

2.1.2 Development of specific training procedures for personnel in charge of managing requests for access to personal data from public authorities, which should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA.

- The training procedures should include the requirements of EU law as to access by public authorities to personal data, in particular as following from Article 52(1) of the Charter of Fundamental Rights.
- Awareness of personnel should be raised in particular by means of assessment of practical examples of public authorities' data access requests and by applying the standard following from Article 52(1) of the Charter of Fundamental Rights to such practical examples.

- Such training should take into account the particular situation of the Processor, e.g. legislation and regulations of the third country to which Processor is subject to, and should be developed where possible in cooperation with Customer.

2.2 Transparency and accountability measures

- Regular publication of transparency reports or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by local law.

2.3 Organizational methods and data minimization measures

2.3.1 Already existing organizational requirements under the accountability principle, such as the adoption of strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures.

- Data minimization should be considered in this regard, in order to limit the exposure of personal data to unauthorized access.
- For example, in some cases it might not be necessary to transfer certain data (e.g. in case of remote access to EEA data, such as in support cases, when restricted access is granted instead of full access; or when the provision of a service only requires the transfer of a limited set of data, and not an entire database).
- In the case at hand, the Parties will implement this as follows: confidentiality obligations of personnel; acknowledgment of acceptable uses of data and technologies; defined roles and responsibilities; security and privacy training; and procedures for onboarding, offboarding, and changes in job duties.

2.3.2 Development and implementation of best practices by both Parties to appropriately and timely involve and provide access of information to their respective data protection officers, if existent, and to their legal and internal auditing services on matters related to international transfers of personal data.

2.4 Others

- Adoption and regular review by Processor of internal policies to assess the suitability of the implemented complementary measures and identify and implement additional or alternative solutions when necessary, to ensure that an essentially equivalent level of protection to that guaranteed within the EEA of the personal data transferred is maintained.

3. Additional Contractual Measures

3.1 Transparency obligations

3.1.1 Processor declares that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data, (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require Processor to create or maintain back doors or to facilitate access to personal data or systems or for Processor to be in possession or to hand over the encryption key.

3.1.2 Processor will verify the validity of the information provided for the TIA questionnaire on a regular basis and provide notice to Customer in case of any changes without delay. Clause 14(e) SCC shall remain unaffected.

3.2 Obligations to take specific actions

- In case of any order to disclose or to grant access to the personal data, Processor commits to inform the requesting public authority of the incompatibility of the order with the safeguards contained in the Article 46 GDPR transfer tool and the resulting conflict of obligations for Processor.

3.3 Empowering data subjects to exercise their rights

- Processor commits to fairly compensate the data subject for any material and non-material damage suffered because of the disclosure of his/her personal data transferred under the chosen transfer tool in violation of the commitments it contains.
- Notwithstanding the foregoing, Livery Video shall have no obligation to indemnify the data subject to the extent the data subject has already received compensation for the same damage.
- Compensation is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Livery Video’s infringement of the GDPR.

APPENDIX 4: Shared Responsibility Model

It is important to understand the shared responsibility model of Livery. The responsibilities vary depending on the type of agreement between the parties. In case of the Livery Platform 4 stakeholders are involved; Cloud Provider, Livery, the Customer and the End-User. The following table shows how the responsibility is shared between the parties.

Responsibility	Customer Model	Bring your own data	Partner Agreement
Last-mile delivery	End-User	End-User	End-User
Device Compliance	Customer	Customer	Customer
Application Configuration	Customer	Customer	Customer
Usage & Compliance Policy	Customer	Customer	Customer
User Account and Access management	Customer	Customer	Customer
Tenant Management & Configuration	Livery	Livery	Customer
Platform Compatibility Validation	Livery	Livery	Livery
Customer data Encryption & Integrity	Livery	Livery	Livery
Platform Management & Configuration	Livery	Livery	Livery
Compute	Shared	Shared	Shared
Video Data Delivery	Cloud provider	Customer	Cloud provider
General Data Delivery	Cloud provider	Cloud provider	Cloud provider
Data Storage	Cloud provider	Cloud provider	Cloud provider
Host Infrastructure	Cloud provider	Cloud provider	Cloud provider