Agreement on Commissioned Processing of Personal Data

according to Art. 28 EU-GDPR

The Parties have entered into a contract which provides that the Customer (hereinafter referred to as the "Controller") will use services of TV1 GmbH, Beta-Straße 9a, 85774 Unterföhring (hereinafter referred to as the "Processor").

To this extent, the Controller commissions the Processor with the processing of personal data on behalf of the Controller pursuant to Article 28 of the EU General Data Protection Regulation 2016/679 (GDPR for short).

This agreement on commissioned processing of personal data regulates the conditions to be complied with and ensured by the Processor when processing personal data on behalf of the Controller. It is concluded electronically by the Controller accepting its provisions as part of an online order. It does not require the signature of the Controller.

The definitions of Article 4 of the GDPR apply.

1. Subject and Duration of Processing

The subject of this Agreement is the performance of the following tasks by the Processor:

Provision of the audio/video streaming platform Video.Taxi.

The commissioned processing begins on 20.09.2022 and

☒ runs for an indefinite period.
☐ ends on DD.MM.YYYY.

2. Categories of Personal Data

Categories of personal data processed by the Processor on behalf of the Controller:

Data related to individuals who receive a Video.Taxi user account:

☒ Identifiers (e.g. name, IP address).
☒ Contact data (e.g., e-mail address).
☒ Address data (e.g., street, postal code)
☒ Bank account data (e.g., IBAN, BIC)
☒ Data on websites and social media accounts associated with the user account
☒ Data on smartphones associated with the user account
☒ Data from support processes and written communication with TV1 (e.g., chat messages, emails).

Data associated with end users:

☒ Identifiers (e.g., name, IP address).
☒ Contact details (e.g., e-mail address).
☒ Data related to transactions (e.g., product name, date of purchase, access code, date of use of an access code)
☒ Statistical data related to access and use of audio/video content.

Data related to individuals whose image, text, or voice is included in content provided via the Video.Taxi platform:

☒ Image data (video)
☒ Voice data
☒ Text data (e.g., chat posts).

Data related to individuals participating in live formats offered via the Video.Taxi platform (e.g., Studio Session):

☒ Identification features (e.g., name, IP address).
☒ Image data (video)
☒ Voice data
☒ Text data (e.g., chat posts)

3. Purpose of Collection, Processing and Use

Purpose of the collection, processing and use of the aforementioned personal data:

Technical provision of the Video.Taxi platform for the transmission of events, administration and delivery of content (including verification of the legitimacy of end users) and evaluation of access and usage to ensure quality of service, as well as billing and creation of access or usage evaluations, if applicable.

4. Categories of Data Subjects

Data subjects are:

☒ Persons employed by the responsible party for the customer-side management of the streaming offers, who are given a Video.Taxi user account for this purpose.
☒ Legitimate users of the audio/video content provided by the responsible party via the Video.Taxi platform ("end users")
☒ Persons whose image, text or speech is included in content provided via the Video.Taxi platform
☒ Persons who participate in live formats offered via the Video.Taxi platform (e.g. Studio Session)

5. Correction, Deletion, Blocking and Return of Data

(1) The Processor shall only correct, delete or block data processed within the scope of the order in accordance with the contractual agreements made or as instructed by the Controller.

(2) At the latest upon termination of the contractual relationship, or beforehand upon request by the Controller, the Processor shall return to the Controller all personal data, documents handed over to it in connection with the contract and processing and usage results produced or, with the prior consent of the Controller, destroy them in accordance with data protection requirements and provide evidence thereof.

(3) Documentation that serves as proof of proper data processing shall be retained by the Processor in accordance with the respective retention periods beyond the end of the contract. The Processor may hand over such documentation to the Controller at the end of the contract for the purpose of discharging the Controller.

(4) The contracting parties mutually undertake to maintain confidentiality about the data disclosed in connection with the order, even beyond the end of the contractual relationship.

6. Obligations of the Processor

(1) The Processor undertakes to strictly maintain confidentiality during processing and to process Personal Data exclusively as contractually agreed or as instructed by the Controller, unless the Processor is legally obliged to perform a specific processing. If such obligations exist for it, the Processor shall notify the Controller of them prior to the Processing, unless the notification is prohibited by law. Furthermore, the Processor shall not use the data provided for processing for any other purposes, in particular for its own purposes.

(2) The Processor warrants that the persons employed by it for processing have been familiarized with the relevant provisions of data protection and this Agreement prior to the start of processing. Corresponding training and awareness-raising measures shall be repeated on an appropriate regular basis. The Processor shall ensure that persons deployed for commissioned processing are appropriately instructed and monitored on an ongoing basis with regard to compliance with data protection requirements and that they comply with the statutory provisions on data protection as well as the rules resulting from this contract, such as binding of instructions and purpose limitation.

(3) Persons who may obtain knowledge of the data processed in the order shall undertake in writing to maintain confidentiality, unless they are already subject to a relevant confidentiality obligation by law.

(4) The Processor confirms that it is aware of the relevant general data protection regulations. It shall observe the principles of proper data processing and shall ensure proper data processing by means of regular checks.

(5) In connection with the commissioned processing, the Processor shall support the Controller in complying with the obligations set forth in Articles 32 to 36 of the GDPR, including the performance of a data protection impact assessment, as well as in creating and updating the list of processing activities pursuant to Article 30 of the GDPR. All required information and documentation shall be kept available and provided to the Controller, without undue delay, upon request.

(6) If the Controller is subject to an inspection by supervisory authorities or other bodies or if data subjects assert rights against the Controller, the Processor undertakes to support the Controller to the extent necessary, insofar as the processing on behalf is affected.

(7) The Processor may only provide information to third parties or the Data Subject, including the disclosure of personal data, with the prior consent of the Controller. The Processor shall immediately forward any inquiries addressed directly to it to the Controller.

(8) A data protection officer has been appointed by the Processor. The e-mail address datenschutz@tv1.eu can be used to contact the data protection officer directly. Changes to the contact data of the data protection officer shall be communicated to the Controller for the purpose of direct contact.

(9) As a matter of principle, commissioned processing takes place within the EU or the EEA. Any relocation to a third country may only take place with the consent of the Controller and under the conditions contained in Chapter V of the GDPR.

(10) If the Processor is not established in the European Union, it shall appoint a responsible contact person in the European Union pursuant to Article 27 of the GDPR. The contact details of the contact person as well as any changes in the person of the contact person shall be notified to the Controller without undue delay.

7. Subcontracting

(1) The commissioning of subcontractors or the involvement of freelancers by the Processor shall require the prior consent of the Controller. In the event of consent being granted, the Processor undertakes to pass on the provisions and obligations set out in this Agreement to the subcontractors and freelancers and to ensure that the Controller also has the right of disposal and the right of control over them in accordance with the contractual provisions set out herein. This shall apply in particular to control and inspection rights of the Responsible Party also directly vis-à-vis the Subcontractor.

(2) Upon request, the Processor shall provide the Controller with information about the essential contractual content of the subcontracting relationship and the implementation of the data protection-relevant obligations in the subcontracting relationship, if necessary by inspecting the relevant contractual documents. The Processor may censor those parts of the contractual documents that are not necessary for data protection monitoring.

(3) Services which the Processor uses from third parties as an ancillary service to support the execution of the order shall not be deemed to be a subcontracting relationship within the meaning of this provision. This includes, for example, telecommunication services, maintenance and user services (provided that no access to data of the Controller can take place), cleaning or testing services.

(4) The commissioning of subcontractors who perform processing operations on behalf of the Processor not exclusively from the territory of the EU or the EEA shall only be possible if the conditions set forth in Chapter 6 (9) and (10) of this Agreement are observed. In particular, it is only permitted to the extent and as long as the subcontractor provides adequate data

protection guarantees. The Processor shall inform the Controller of the specific data protection guarantees offered by the subcontractor and how proof thereof can be obtained.

8. Technical and Organizational Measures

(1) The Processor shall implement and document the technical and organizational measures listed in Annex 2 to this Agreement prior to the start of data processing and hand them over to the Controller for inspection upon request. The measures described in Annex 2 are defined as binding. They define the minimum owed by the Processor.

(2) The implementation of and compliance with all technical and organizational measures required for this order in accordance with Art. 32 GDPR shall also be fulfilled by the Processor beyond the measures specified in Annex 2.

(3) The technical and organizational measures are subject to technical progress and further development, and may be updated in the course of the contractual relationship in accordance with further technical and organizational development in the area of the Processor. In doing so, the Processor shall not fall below the security level of the specified measures.

(4) If fundamental changes are made to the technical and organizational measures, these shall be coordinated with the Controller. The changes shall be recorded in writing and Annex 2 shall be adapted accordingly by the Processor. However, coordination shall not be required if the changes lead to an improvement in the level of data protection agreed under this Agreement on Data Processing by Order and the Controller is informed of these changes. Annex 2 shall be adapted accordingly.

(5) Insofar as the measures taken do not or no longer meet the requirements of the Controller, the Processor shall notify the Controller without undue delay.

(6) Insofar as Personal Data are processed in private residences or in the context of teleworking, the Processor shall ensure compliance with any necessary special data protection measures within the meaning of Art. 32 GDPR.

(7) The Processor shall provide the Controller with evidence of the implementation of and compliance with the technical and organizational measures. For this purpose, it may also submit current test certificates, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors) or suitable certification through IT security or data protection audits.

(8) Taking into account the type of processing commissioned and the information available to the Processor, the Processor shall adequately assist the Controller in fulfilling its responsibilities under Articles 32 to 36 GDPR (concerning security of processing, notification obligations, data protection impact assessments and consultations with the relevant supervisory authority).

9. Control Rights of the Controller

(1) The Controller shall be entitled to convince itself or through commissioned third parties of the compliance with the technical and organizational measures taken by the Processor, also on site, prior to the start of data processing by the Processor and thereafter on a regular basis.

(2) In the event of on-site inspections, the Controller shall take into account the Processor's operational procedures and notify inspections at least two weeks in advance. If the Processor violates its contractual obligations under this Agreement, violates provisions of data protection law, or if a statutory regulation provides for a shorter period, the advance notification obligation shall be reduced to 24 hours.

(3) The Processor shall be obliged to support the Controller in carrying out the controls to the best of its ability. The Processor undertakes to provide the Controller, upon request, with the information and evidence necessary to comply with the Controller's obligation to carry out checks on the processing of personal data.

10. Notification in the Event of Breaches by the Processor

(1) The Processor and the Controller shall inform each other without undue delay if disruptions, irregularities or suspected data protection breaches occur. The Parties shall make all reasonable efforts to remedy any violations without undue delay.

(2) The Processor shall in all cases notify the Controller if violations of the Controller's personal data protection regulations or of the specifications made in the order have occurred by the Processor or the persons employed by the Processor.

(3) It is known that according to Art. 33 and/or 34 of the GDPR, information obligations may exist in the event of a data protection breach. Therefore, such incidents (including loss, unauthorized publication or unauthorized access to data) must be reported to the Controller without delay and within 48 hours at the latest, regardless of causation. This shall also apply in the event of serious disruptions to operations or suspected other violations of the Controller's personal data protection regulations. The Processor shall, in consultation with the Controller, take appropriate measures to secure the data and to mitigate any possible adverse consequences for Data Subjects. Insofar as the Controller is subject to obligations pursuant to Art. 33 and/or 34 of the GDPR, the Processor shall support the Controller in this regard.

11. Authority to Issue Instructions by the Controller

(1) The Processor shall be strictly bound by the instructions of the Controller at all stages in the execution of the order and the processing of personal data of the Controller. The Controller reserves a comprehensive right to issue instructions on the type, scope and procedure of data processing, which it may specify by means of individual instructions.

(2) The Processor shall notify the Controller without delay if it believes that an instruction violates data protection regulations. The Processor shall be entitled to suspend the implementation of the corresponding instruction until it has been confirmed or amended by the Controller - after having been notified.

12. Liability

The regulations under point 14 of the terms of use apply. Aside from this, reference is made to Art. 82 GDPR.

Final Provisions

Upon conclusion of this Agreement, any (framework) regulations on commissioned data processing concluded between the Parties shall be replaced by this Agreement. The subject matter as well as the description of the data processing commissioned in each case shall remain in force for the respective specified term of the agreement.

Amendments to this Agreement must be made in writing. (Oral) collateral agreements do not exist.

Should any of the above provisions be or become invalid or incomplete in whole or in part, this shall not affect the validity of the remaining provisions. The parties undertake to replace the invalid or incomplete provision with a valid provision that comes as close as possible to the economic purpose and intention of the parties.

The description of the technical and organizational measures according to Annex 2 is an integral part of this agreement.

Munich, 20.09.2022

Processor (Contractor)
TV1 GmbH

Annex 1: Subcontracting Relationships

Relevant subcontracting relationships according to Chapter 7 of this agreement that are relevant in the context of this commissioned processing:

Company Name	Headquarters in	Object of Relationship:
Braintree Payments	21 Rue de la Banque 75002 Paris France	Payment Processing
KIM Keep In Mind GmbH	Bruno Buozzi Str. 12 39100 Bolzano Italy	Software Development, Support
Zendesk	Schönhauser Str. 3-5 10178 Berlin Germany	Support Tool
AppSignal B.V.	Rietwaard 4 5236 WC 's Hertogenbosch The Netherlands	Website Error Tracking Tool
Pipedrive Deutschland GmbH	Julie-Wolfthorn-Straße 1 10115 Berlin Germany	CRM Tool
Amazon Web Services EMEA SARL *)	Marcel-Breuer-Str. 12 80807 Munich Germany	Cloud Services (including Storage)
Betaeins GmbH *)	Beta-Straße 1 85774 Unterföhring Germany	Server Hosting (Data Center)

The subcontractors marked with *) shall at no time have access to personal data of customers (persons with user accounts) and end users. The order control on the part of TV1 in these cases refers to ensuring adequate implementation of appropriate technical and organizational measures to prevent unauthorized access to the content provided via the Video.Taxi platform, including any personal data it may contain.

Annex 2: Technical and Organizational Measures (TOM)

according to Art. 32 EU-GDPR

This annex describes the technical and organizational measures implemented uniformly by TV1 GmbH to meet legal and contractual data protection requirements.

The measures described in numbers 1 to 13 serve the purpose of:

- encrypting or pseudonymizing personal data where necessary (see, among others, 6 to 8),
- ensuring the confidentiality, integrity, availability and resilience of systems and services in connection with the commissioned processing of personal data on a permanent basis (see, among others, 1 to 10),
- being able to quickly restore the availability of and access to personal data in the event of a physical or technical incident (see 11 below); and
- regularly reviewing, assessing and evaluating the effectiveness of all technical and organizational measures to ensure the security of processing (see, among others, 12 and 13).

Certification: The Information Security Management System (ISMS) of TV1 GmbH is certified according to the International Requirements Standard ISO/IEC 27001.

(1) Admittance Control

All access rights (both for access to IT systems and data and for admittance to buildings and rooms) are assigned according to the principle that employees and third-party users are only granted the level of access they need to perform their activities (minimum principle).

Access rights are granted according to defined (role-based) authorization profiles. The access rights granted are reviewed regularly. Rights that are no longer required are withdrawn promptly.

Access to networks and network services is restricted by technical and physical measures. Access to wireless corporate networks that allow access to personal data is protected by personalized authentication (PKI, IEEE 802.1x). This applies analogously to wired access, unless it is from a secure area sufficiently protected and controlled by physical access control measures.

(2) Entry Control

Physical security areas (security zones) are defined on the basis of information security and data protection requirements and protected against unauthorized entry by appropriate physical protection measures. The zone concept distinguishes between public areas, controlled areas, restricted/internal areas, and high-risk zones. Zones are defined based on the protection needs of the information assets housed or accessible within them.

Depending on the specific zone classification, selected or all of the following security features are implemented: entry restriction through personalized access medium, video surveillance and door-open sensors at entry points, motion detection, privacy screens or view guards on potentially confidential information, photography prohibition.

For dealing with visitors and deliveries, procedures are used to prevent unauthorized persons from entering security areas.

(3) Access Control

All data processing systems are equipped with a secure authentication mechanism (password protection, in some cases multi-factor authentication).

Defined and traceable procedures are used to authorize access to information, taking into account the minimum principle. Separate procedures exist for granting access authorizations for particularly privileged systems (e.g., systems or applications used to control or administer critical processes or also to manage other access rights).

For authentication on data processing systems (IT systems), secure passwords are used that have sufficient length and complexity according to the state of the art to be robust against dictionary attacks (e.g., combination of upper and lower case letters, digits and special characters, no strings of consecutive letters or digits). Passwords must not be based on factual information that can be easily guessed by others.

Passwords shall be changed regularly. In doing so, the changed password must not match or contain a password that has been used in the past.

A "Clear Desk & Screen Policy" has been implemented: when leaving a workstation, all computers in use must be locked (screen lock). In case of inactivity, the screen lock is automatically activated after a maximum of 10 minutes. Documents that may contain confidential information must not be kept open and unattended on desks or in other freely accessible storage areas.

(4) User Control

All employees must attend mandatory basic training on information security and data privacy on an annual basis. Attendance at this training is recorded and its effectiveness is validated by an audit. New employees are familiarized with the essential information security and data protection regulations relevant to them at the start of their employment or assignment.

User activities, including logon attempts to data processing systems (IT systems), are logged to the extent required.

User accounts that can be used to access personal data as part of commissioned processing must be personalized and may not be shared by more than one person.

Central monitoring is carried out to monitor utilization with threshold-based alerting (e.g. CPU, memory) and error monitoring. In addition, event information from IT solutions in use is evaluated.

Administrative activities on IT systems (such as changes to system configurations) are logged. Configuration files are historized, backed up and checked regularly and as required.

(5) Separation Control

It is ensured that personal data collected for different purposes are not mixed in their processing. To this end, client-capable systems are used where necessary, or client systems are physically or logically separated. In server environments, functions are separated.

(6) Control of Data Carriers and Mobile Devices

Data carriers containing personal data shall be stored in secure locations that exclude access to the data carriers by unauthorized persons.

Personal data stored on mobile devices and data carriers (including laptops, smartphones, USB sticks) must be encrypted. The use of any type of Internet/cloud storage for (temporary) storage of such data is prohibited. Confidential data will never be stored on private storage media or end devices.

Data that is no longer required will be deleted. Electronic storage media and paper documents that are no longer required will be disposed of or destroyed / rendered unusable in such a way that it is no longer possible to gain knowledge of the data stored or contained on them.

The use of mobile devices is restricted and regulated. If personal data is accessed via mobile devices, suitable measures are taken to ensure that the devices cannot be used by unauthorized persons, for example in the event of loss or theft. All mobile devices used for business purposes are configured in such a way that they are protected by a query for a complex PIN (at least 6 digits/characters) in the lock screen. The lock screen is automatically switched on during inactivity. The corresponding mobile devices must never be left unattended. Modifications to the operating system software / firmware are prohibited. Security-relevant updates and patches are applied automatically. The devices are subject to comprehensive Mobile Device Management (MDM), which technically implements these and other restrictions, specifications and measures.

(7) Pseudonymization and Anonymization

Measures for pseudonymization or anonymization of personal data are implemented to the extent necessary. Data in development environments used for testing purposes is anonymized or pseudonymized wherever possible. Data on the use of websites that is evaluated to generate usage statistics is anonymized.

(8) Transmission and Forwarding Control

Mechanisms for controlling data traffic and communication links and for monitoring and logging activities on the network are established to the required extent.

A firewall solution and intrusion detection and prevention systems (IDS / IPS) are in place. Data traffic analysis includes checking the validity of certificates for encrypted communications, checking accessed Internet resources (comparison with blacklists and whitelists), and pattern recognition to identify potential malicious code. Potentially malicious Internet data communications are blocked using gateway antivirus, botnet and geo-IP filters, among other measures.

When personal data is transmitted via public communication networks, secure end-to-end encryption of the communication is ensured. When establishing secure connections (VPN tunnels) with full-spectrum access to the company's own IT resources via public networks, two-factor authentication is always used. If the exchange of confidential authentication information is required, this is done via a different communication path than the actual data transmission.

When transporting personal data stored on data carriers, the use of encryption, among other things, ensures that the data is protected against unauthorized access, manipulation or loss. After transport, the data is deleted from the storage media used for transport if it is no longer required to be on them.

Paper printouts and exports of confidential data from their source system will be avoided whenever possible. Hard copies and electronic exports of confidential information leaving the business premises will be handled with special care, taking into account the relevant confidentiality level - with the aim of preventing disclosure, loss and unauthorized copying. As soon as a paper printout is no longer required, it is destroyed. Electronic data exports that are no longer required are deleted again from the respective storage location and any transport data carrier used.

9) Input Control

Measures for subsequent verification of whether and by whom data has been entered, changed or removed (deleted) have been implemented to the extent required. In systems used to collect and process personal data, accesses are categorized and automatically recorded. The integrity of the log information is guaranteed by technical and organizational measures.

(10) Availability Control

A redundant design of communication and data processing systems (IT systems) and supporting utilities has been implemented to the required extent. Significant parts of the data center infrastructure are geo-redundant (fallback data center). An uninterruptible power supply (UPS) and high-availability Internet connection with automatic failover have been implemented at all relevant locations. Server and storage systems are designed redundantly (including redundant power supply units, disk mirroring). Automatic load balancing and failover are implemented for virtualized server systems.

(11) Restorability

Data backups of data files and operating system images are performed to the extent required for order processing and with the aim of preventing the loss of personal data in the event of a technical defect or human error. Data backups are performed for network drives, servers in productive operation, as well as development and test servers, and the performance is recorded (logged) and monitored. The restoring of data backups is tested regularly.

Processes or procedures for handling disruptions to IT systems and for restoring systems after a disruption have been established to the extent required.

Business continuity management (BCM) includes activities for business process impact analysis (BIA), definition and application of measures to ensure business continuity, taking into account information security and data protection aspects, as well as tests and reviews of the effectiveness of the measures introduced. A business process impact analysis is prepared or reviewed at least annually on the basis of the key business processes.

(12) Contract Control

The selection of subcontractors, if contractually agreed, is carried out with the objective of ensuring that there is no increased risk to compliance with data protection objectives. Commissioned data processing in accordance with instructions shall be ensured.

Depending on their role and the scope of access to confidential or personal data, subcontractors must, among other things, take note of and comply with regulations on secrecy / confidentiality and data protection (e.g., confidentiality / non-disclosure agreement (NDA), agreement on commissioned processing of personal data) as well as a Supplier Information Security Policy.

In the case of security-critical subcontractors, service providers or suppliers, the following reporting and auditing requirements are implemented: at least quarterly evaluation of contractually agreed reports (e.g., security events/incidents, availability statistics) as well as supplier audits every 2 years using a self-assessment questionnaire, with an additional on-site visit if necessary.

(13) Review, Assessment and Evaluation

Information on possible technical vulnerabilities or errors in data processing systems (IT systems) is evaluated at regular intervals and appropriate measures are initiated. Comprehensive patch management is implemented for both operating systems and software applications used.

Data processing systems (IT systems) are checked regularly to the extent required and after changes to ensure that they are functioning properly.

TV1 GmbH's information security management system (ISMS) is certified in accordance with the international requirements standard ISO/IEC 27001. The scope of the certification includes development, operation, production, monitoring and support for live and on-demand streaming services of TV1 GmbH. No exclusions of the reference measures (controls) were made as part of the Statement of Applicability. To maintain certification, annual audits are carried out to the prescribed extent by the testing service provider TÜV SÜD Management Service.

In addition to external audits and controls, TV1 GmbH implements an internal audit program that includes regular system audits, process audits, IT security audits and data protection audits and controls.