FairReplay Data Processing Agreement v 1.0. - November 2023

PREAMBLE AND INTRODUCTORY REMARKS

This **FairReplay Data Processing Agreement** and its **Appendices** reflects the parties' agreement with respect to the **Processing** of **Personal Data** by **DATASTAT Svetovanje in izdelava statističnih podatkov in multimedijskih vsebin d.o.o.** (as the **Processor**) on behalf of the **Customer** (as the **Controller**) in connection with the **Customers'** use of the **FairReplay Service**, whereby all bolded terms are further defined below.

This **DPA** is supplemental to, and forms an integral and indispensable part of the **Agreement** (i.e. the **FairReplay Terms of Service** https://www.fairreplay.com/terms/), which applies to the use of the **FairReplay Service** by the **Customer**.

In case of any conflict or inconsistency between the terms and clauses of this **DPA** and the terms and clauses of the **Agreement**, this **DPA** will take precedence over the terms and clauses of the **Agreement** to the extent of such conflict or inconsistency.

Terms not otherwise defined in this **DPA** will have the meaning as set forth in the **Agreement**.

All enquiries regarding this **DPA** may be directed at dpo@datastat.si.

1 THE APPLICATION OF THIS DPA

1.1 This **DPA** shall be deemed as validly concluded between:

- **DATASTAT Svetovanje in izdelava statističnih podatkov in multimedijskih vsebin d.o.o.**, Vojkova cesta 58, 1000 Ljubljana, Slovenia, Company Registration Number: 3392392000, VAT ID Number: SI 26084279, the owner and supplier of the **FairReplay Service** (hereinafter: *"**we**"*, *"**us**"*, *"**our**"*, *"**Provider**"* or "***Processor***") and which can be reached at dpo@datastat.si, and;

- you as the **Client** (hereinafter also: **you**, **your**, **User**, **Customer, Controller**), namely the legal entity that shall be identified as the registered **User** of the **Service** when you, the natural person acting as the duly authorised individual representing said entity, register a registered **User** account. The aforementioned also relates to any and all **Personnel** and **Affiliates.**

- whereby the **Processor** and **Controller** may be hereinafter jointly referred to as the **Parties**.

1.2. Before your use of the **Services**, you are asked to dully review, understand and get acquainted with the content of both this **DPA** and the **Agreement**.

1.3. Any reference to this **DPA** includes its **Appendices.**

1.4. The **Provide**r may host the list of **Approved Subprocessors** from **Appendix 1** online and communicate this to the **Customer**, whereby it shall be deemed that the online list represents the last version of the list from **Appendix 1** and shall have legal effect.

2 CHANGES

2.1 We may make changes to this **DPA** at any time by notifying you of the change by email and proposing the conclusion of an amendment to this **DPA**. Unless stated otherwise, any change shall take effect from the date of the concluded amendment to this **DPA**. You are responsible for ensuring you are familiar with the last version of this **DPA**.

3 INTERPRETATION

In this **DPA**:

FairReplay Terms of Service (also called **Agreement** or **Terms**) shall mean the underlying agreement that has been entered into by the parties and which governs the setting-up, use and access of/to the **Service** and under which certain **Personal Data** need to be processed in accordance with this **DPA**. The legally binding version of the **Agreement** can be found at https://www.fairreplay.com/terms/ at any time, whereby the **Agreement** represents a set of template clauses that form an agreement that is entered into when you register a **User** account.

Applicable legislation shall mean but not be limited to the European Union's General Data Protection Regulation (2016/679) (hereinafter: ***"GDPR"***) as well as any and all applicable EU and national laws and other statutes, rules, regulations and codes, as they may apply to the use and the consequences of use of the **Service.**

FairReplay Service (also called **Services** or **Service**) shall mean the software programs and online platforms with the core functionalities as described in the **Agreement** and as defined on the https://www.fairreplay.com/ website as well as any related services that the **Provider** performs for the **Customer** under the **Agreement** and the respective underlying infrastructure, whereby provision of the **Service** requires the processing of certain **Personal Data** for its normal and intended functioning, as outlined below.

FairReplay Data Processing Agreement (also called **DPA**) shall mean this legal agreement under which the **Provider** shall be deemed as the **Processor** and you shall be deemed as the **Controller** of any and all **Personal Data** that shall be sent, transmitted, transferred or otherwise processed by the **Provider** directly in connection with the performance of the **Service**. This **DPA** forms a supplemental, integral and indispensable part of the **Agreement** and your use of the **Services**, whereby this **DPA** is subject to the provisions of Article 28 of the **GDPR**.

Consent shall mean any freely given, specific, informed and unambiguous indication of the **Data subject**'s (i.e. **End User**'s) wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of **Personal Data** relating to him or her, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**.

Customer Affiliate shall mean in respect of the **Customer** and his legal entity, any other legal entity or private person controlling the **Customer** or being controlled by the **Customer**, or acting under the direct influence or instructions of the **Customer**, whereby "being controlled by" shall mean the possession, directly or indirectly, solely or jointly with another person, of power to direct or cause the direction of the management or policies and cations of a legal or natural person (whether through the ownership of securities, other shareholders, partnership or ownership interest, by establishing total or partial identity of individuals in management, by contract or otherwise).

Controller shall mean the legal person which, alone or jointly with others, determines the purposes and means of the processing of **Personal Data**, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**. Please note, that even in the event that you are not in fact the **Controller** of the **Personal Data** that you are using or wish to use in connection with the **Service**, you expressly warrant and represent to the **Provider**, that you have the necessary legal grounds and have obtained the required consent for the processing of the **Personal Data** of the **End Users** in connection with your use of the **Service** from the actual **Controller** of said **Personal Data**. In the context of this **DPA**, **Controller** shall mean you, the client.

Controller Personal Data shall mean any **End User Personal Data** or any other **Personal Data**, for which the **Controller** may be deemed as the "controller" under **Applicable legislation** and that the **Provider** or **Subprocessor** shall **Process** pursuant to or in connection with the **Agreement** and this **DPA**.

Data processing (also **Processing**) means any operation or set of operations which is performed on **Personal Data** or on sets of **Personal Data**, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In the context of this **DPA**, the **Provider** shall **Process** the **End User Data** for which the **Customer** is deemed as the **Controller** in order to provide the **Service**, as outlined below.

End User (also **Data Subject**) shall mean a natural person whose **Personal Data** is processed in connection with the **Service**. **End Users** are generally sport event participants and other individuals whose personal data was processed (i.e. added, stored, shown and otherwise processed as described below) in connection with the **Service** by the **Controller** or his affiliates.

European Economic Area (also called **EEA**) shall mean the EU Member States as well as Iceland, Liechtenstein, and Norway.

Provider shall mean **DATASTAT Svetovanje in izdelava statističnih podatkov in multimedijskih vsebin d.o.o.**, Vojkova cesta 58, 1000 Ljubljana, Slovenia, Company Registration Number: 3392392000, VAT ID Number: SI 26084279 and its employees. In the context of this **DPA**, the **Provider** shall be deemed as the **Processor** of **Personal Data**.

Provider Affiliate shall mean in respect of the **Provider** and its legal entity, any other legal entity or private person controlling the **Provider** or being controlled by the **Provider**, or acting under the direct influence or instructions of the **Provider**, whereby "being controlled by" shall mean the possession, directly or indirectly, solely or jointly with another person, of power to direct or cause the direction of the management or policies and cations of a legal or natural person (whether through the ownership of securities, other shareholders, partnership or ownership interest, by establishing total or partial identity of individuals in management, by contract or otherwise).

Personal Data shall mean any information relating to an identified or identifiable natural person (i.e. **End User** or **Data subject**), whereby an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**.

Personal Data Breach shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**.

Processor shall mean a natural or legal person, public authority, agency or other body which processes **Personal Data** on behalf of the **Controller**, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**. In the context of this **DPA**, the **Provider** shall be deemed as the **Processor** of **Personal Data**.

Processing shall mean an operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Party shall mean either the **Customer** or the **Provider** whereby the term also includes that **Party**'s permitted assigns. The term "parties" shall mean both the **Customer** and the **Provider**.

Privacy policy shall mean the information to be provided to the **Data subject** where **Personal Data** are collected from the **Data subject**, as provided for by Article 13 of the **GDPR** or by any other relevant **Applicable legislation**.

Person includes an individual, a body corporate, an association of persons (whether corporate or not), a trust, a government department, or any other entity.

Personnel includes officers, employees, contractors, and agents of the **Customer** (or **Customer Affiliates**).

Special categories of personal data shall mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Start Date shall mean the date on which this **DPA** was entered into, namely the date the **User** has registered his account.

Subprocessor (or **Contracted Subprocessor**) shall mean any person (including any third party and any **Provider Affiliate**, but excluding an employee of the **Provider** or any of its subcontractors) appointed by or on behalf of the **Provider** or any **Provider Affiliate** to **Process Personal Data** on behalf of the **Provider** in connection with the **Agreement.** The provider may host the list of **Approved Subprocessors** from **Appendix 1** of this **DPA** online, whereby it shall be deemed that the online list represents the last version of said list.

Standard contractual clauses shall mean the latest standard data protection clauses for the transfer of **Personal Data** to **Processors** established in countries outside of the **EEA**, where an adequate level of data protection with regards to the **GDPR** is not ensured on a national and systemic level, as described in Article 46 of the **GDPR**.

You hereinafter also: **you**, **your**, **User**, **Customer, Controller, Client**), namely the legal entity that shall be identified as the registered **User** of the **Service** when you, the natural person acting as the duly authorised individual representing said entity, register a registered **User** account. The aforementioned also relates to any and all **Personnel** and **Affiliates.** In the context of this **DPA** you as the **Customer** shall be deemed as the **Controller** of **Personal Data**.

3.2. Words in the singular include the plural and vice versa. Non-bold terms or uncapitalized terms may still hold the meaning of the corresponding term that has been described above.

3.3. A reference to the **Applicable legislation** or statute includes references to regulations, orders or notices made under or in connection with such legislation, statute or regulations and all amendments, replacements or other changes to any of them.

4 CONTRACTUAL INTENT AND TERM

4.1. The Parties seek to implement this **DPA** in order to achieve compliance with the requirements of the **Applicable legislation** as it pertains to the **Processing** of **Personal Data** and especially Article 28 of the **GDPR**, which forms the basis under which this **DPA** is drafted and construed.

4.2. Notwithstanding any other provision relating to the term of this **DPA**, this **DPA** will take effect on the **Start Date** and shall remain in force until the **Provider** has deleted or returned all **End User Personal Data** to the **Controller**, whereby it shall be deemed as automatically terminated.

5. PROCESSING OF CONTROLLER PERSONAL DATA

5.1. **Permitted scope of Processing.**

The **Provider** shall:

- **Process Controller Personal Data** in order to provide the **Service** as stated in the **Agreement** or on the basis of relevant **Controller**'s documented instructions, which shall be deemed as contained herein unless otherwise provided to the **Provider** in writing,

    - comply with any and all **Applicable legislation** in the **Processing** of **Controller Personal Data,**

    - **Process Controller Personal Data** if **Processing** is required under the **Applicable legislation** to which the **Provider** or relevant **Contracted Processor** is subject, in which case the **Provider** shall, to the extent permitted under the **Applicable legislation**, inform the **Controller** of that legal requirement before the relevant **Processing** of such **Personal Data** takes place.

5.2. For the avoidance of doubt, the **Provider** shall only use the **Controller Personal Data** to provide the **Service** and shall not keep, retain, disclose, make available to third parties, sell or otherwise use the **Controller Personal Data** for any purpose other than for providing the **Service** under the **Agreement** as further described in **Appendix 1**.

5.3. The **Controller** instructs the **Provider** and each **Provider Affiliate** (and authorises the **Provider** and each **Provider Affiliate** to instruct each **Subprocessor**) to:

- **Process Controller Personal Data** as necessary for the provision of the **Service** as specified in **Appendix 1**,

- transfer **Controller Personal Data** to any country or territory as reasonably necessary for the provision of the **Services** and consistent with the **Agreement** if such territory is in the **EEA**, as specified in sections 8 and 14.

5.4. The **Controller** warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 5.3. for all **Controller Personal Data** and on behalf of each relevant **Controller Affiliate**.

5.5. **Appendix 1** to this **DPA** sets out certain information regarding the **Contracted Processors' Processing** of the **Controller Personal Data** as required by Article 28 of the **GDPR** (and, possibly, equivalent requirements of other **Applicable Legislation**). The **Controller** may make reasonable amendments to **Appendix 1** by written notice to **Provider** from time to time that the **Controller** considers necessary to meet those requirements and may host the list of approved **Subprocessors** online, whereby it shall be deemed that the online list represents the last approved version of the list from **Appendix 1**.

6. Provider and Provider Affiliate Personnel

6.1. The **Provider** and each **Provider Affiliate** shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any **Contracted Processor** who may have access to the **Controller Personal Data**, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant **Controller Personal Data**, as strictly necessary for the purposes of the **Agreement**, and to comply with **Applicable legislation** 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.

7. Security and the keeping of records

7.1. 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, the **Provider** and each **Provider Affiliate** shall in relation to the **Controller Personal Data** implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32 of the **GDPR**.

7.2. The list of technical and organisational measures that the **Provider** and each **Provider Affiliate** offers the **Controller** under this **DPA** is included in **Appendix 2**.

7.3. Prior to concluding the **Agreement** and this **DPA**, the **Controller** is required to review and analyse the contents of **Appendix 2** with regards to the technical and organisational measures and other security commitments which the **Provider** offers in connection with the provision of the **Service**.

7.4. In assessing the appropriate level of security, the **Provider** and each **Provider Affiliate** shall take into account the particular risks that are presented by **Processing Personal Data** and in particular the risk of a **Personal Data Breach**. The **Controller** understands and agrees that it is his sole responsibility to consider if the technical and organisational measures from **Appendix 2** meet his security needs and obligations with regards to **Controller Personal Data** and the **Applicable legislation**.

7.5. Regarding the aforementioned, the **Controller** understand and agrees, that he is solely responsible for his use of the **Service**, and is asked to put in place and maintain his own technical and organisational measures, which must include industry level best practises such as:

- making copies (i.e. backing up) all **Controller Personal Data** prior to use with the **Service**,
- practising safe and secure usage of the **Service** and the user account / password of of the **Customer** (secure keeping of account authentication credentials),
- securing systems and devices which are used to access or interact with the **Service**.

7.6. The **Provider** and **Provider Affiliates** take no responsibility regarding the processing, storage and protection of **Controller Personal Data** outside of the **Service** and the subsystems connected to the **Service** (which includes, but is not limited to, the access and storage of **Controller Personal Data** on the servers of the **Controller** or a third party (such as an approved **Subporcessor**), the transferring of **Controller Personal Data** to third parties, the distribution of account authentication credentials to third parties, etc.).

7.7. The **Controller** understands and agrees that by concluding the **Agreement** and this **DPA**, the technical and organisational measures from **Appendix 2** as well as other aspects of the security are deemed as appropriate with regards to the risk posed to the **Data Subjects** and the **Controller Personal Data**.

7.8. The **Provider** shall, to the best of his ability, keep records (i.e. log files) regarding the **Processing** of **Controller Personal Data**, and shall ensure that the records are sufficient to meet the communicated compliance requirements of the **Controller**. The **Provider** shall also provide said records to the **Controller** upon his written request.

8. Subprocessing

8.1. The **Controller** specifically authorises and generally agrees with the **Provider** and each **Provider Affiliate** appointing and engaging **Subprocessors** in their own discretion, if such appointment is directly tied to the fulfillment of the **Agreement**, necessary for the provision of the **Service** and in accordance with this section 8.

8.2. The **Provider** and each **Provider Affiliate** may also continue to use those **Subprocessors** already engaged by the **Provider** or any **Provider Affiliate** at the **Start Date**, whereby the **Provider** and **Provider Affiliate** shall be in each case and as soon as practicable required to ensure, that the obligations set out in this section 8 are met by such **Subprocessors**.

8.3. The list of **Subprocessors**, including details regarding their location and **Processing** functions is available in **Appendix 1,** whereby an online version of the list may be made available by the Provider and communicated to the **Customer**. In such situations it shall be deemed, that the online list represents the last version of the list from **Appendix 1** and shall have legal effect.

8.4. Regarding the **Processing** and subprocessing of **Controller Personal Data,** the **Provider** and any **Provider Affiliate** shall only appoint and engage **Subprocessor** through the conclusion of a data processing agreement containing all necessary data protection obligations (or a separate valid legal mechanism), which shall offer the same level of data processing protection that can be found in this **DPA**, to the extent applicable to the nature of the **Services** provided by such **Subprocessors**.

8.5. The **Provider** shall add such newly engaged **Subprocessor** to the online list of **Subprocessors** in reasonable time. The parties hereby agree, that such method of notification is adequate with regards to the **Controller's** right to be notified prior to **Subprocessor** engagement.

8.6. Should the **Controller** or **Controller Affiliate** oppose the engagement and appointment of a new **Subprocessor**, he shall notify the **Provider** within ten (10) business days from the the day when such processor had been added to the list as referred to in the previous point. After that, **Processing** by the **Subprocessor** shall be deemed as accepted by the **Controller** or **Controller Affiliate**.

8.7. Should the **Controller** or **Controller Affiliate** oppose the engagement and appointment of a new **Subprocessor** and notify the **Provider** regarding this (even after the expiration of the period from the previous point), all data processing by such newly appointed **Subprocessor** shall cease and the parties shall seek to find an applicable solution in good faith. If the parties cannot agree on an applicable solution regarding the objection in 150 days, the **Controller** may terminate the **Agreement** in accordance with its provisions.

8.8. The **Provider** may be held liable for obligations subcontracted to the **Subprocessors**, including their acts and omissions under **Applicable legislation**.

9. Data Subject Rights

9.1. Taking into account the nature of the **Processing**, the **Provider** and each **Provider Affiliate** shall assist the **Controller** by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the **Controllers'** obligations to respond to requests to exercise **Data Subject** rights under the **GDPR** and the **Applicable legislation**.

9.2. The **Provider** shall:

- promptly notify the **Controller** if the **Provider** or any **Contracted Processor** receives a request from a **Data Subject** under the **GDPR** and the **Applicable legislation** in respect of **Controller Personal Data** (if such notification is duly transferred to the **Provider**, which is the obligation of the **Contracted Processor**); and
- ensure that he does not respond to such request himself and does so only upon the documented instructions of the **Controller** or the relevant **Controller Affiliate,** notwithstanding situations in which the **Provider** may be required to respond on their own to such request under the **GDPR** or the **Applicable legislation**, in which case the **Provider** shall, to the extent permitted by the **GDPR** or **Applicable legislation**, inform the **Controller** of such legal requirement beforehand.

10. Personal Data Breach

10.1. The **Provider** shall notify the **Controller** within 5 days upon the **Provider** or any **Subprocessor** becoming aware of a **Personal Data Breach** affecting the **Controller Personal Data**, providing the

Controller with sufficient information to allow him to meet any obligations to report or inform the **Data Subjects** of the **Personal Data Breach** under the **Applicable legislation**.

10.2. The **Provider** shall cooperate with the **Controller** and take such necessary commercial steps as are directed by the **Controller** to assist in the investigation, mitigation and remediation of each such **Personal Data Breach**.

11. Data Protection Impact Assessment and Prior Consultation

11.1. The **Provider** and each **Provider Affiliate** shall provide assistance to the **Controller** with any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, which the **Controller** reasonably considers to be required under Article 35 or 36 of the **GDPR** or equivalent provisions of any other **Applicable legislation**, in each case solely in relation to the **Processing of Controller Personal Data** by, and taking into account the nature of the **Processing** and information available to, the **Provider** and the **Contracted Processors**.

12. Deletion or return of Controller Personal Data

12.1. Subject to points 12.2 the **Provider** and each **Provider Affiliate** shall promptly and in any event within 15 (fifteen) business days of the date of termination of the **Agreement** (i.e. termination by either the **Controller** or the **Provider** under the applicable clauses of the **Agreement**) delete and procure the deletion of all copies of those **Controller Personal Data** that are listed as being stored in **Appendix 1**, thereby permanently removing all copies and instances of such data in the **Provider**'s systems. By notifying the **Provider** prior to termination of the **Agreement**, the **Controller** and **Provider** may also arrange for the transfer of such data to the **Controller** prior to deletion.

12.2. The **Provider** and each **Contracted Processor** may retain **Controller Personal Data** to the extent required by **Applicable legislation** and only to the extent and for such period as required by the **Applicable legislation** and always provided that the **Provider** and each **Provider Affiliate** shall ensure the confidentiality of all such **Controller Personal Data** and shall ensure that such **Controller Personal Data** is only **Processed** as necessary for the purpose(s) specified in the **Applicable legislation** requiring its storage and for no other purpose.

13. Audit rights

13.1. The **Provider** and each **Provider Affiliate** shall make available to the **Controller** on request all information necessary to demonstrate compliance with this **DPA**, and shall allow for and contribute to audits, including inspections by the **Controller** or an auditor mandated by the **Controller** in relation to the **Processing** of the **Controller Personal Data** by the **Provider** or the **Contracted Processors**. The Provider and each **Provider Affiliate** shall immediately inform the **Controller** if, in their opinion, an instruction infringes the GDPR or other applicable data protection provisions, this **DPA**, or the **Agreement**.

13.2. The **Controller** or the relevant **Controller Affiliate** undertaking an audit shall give the **Provider** or the relevant **Provider Affiliate** a notice at least thirty (30) business day prior to any audit or inspection being conducted under this section 13 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the **Provider'**s or **Contracted Processors**' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. The **Provider** or a **Contracted Processor** need not give access to its premises for the purposes of such an audit or inspection:

- to any individual unless he or she produces reasonable evidence of identity and authority;
- outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the **Controller** or the relevant **Controller Affiliate**

undertaking an audit has given notice to the **Provider** or the relevant **Provider Affiliate** that this is the case before attendance outside those hours begins; or

- for the purposes of more than one audit or inspection, in respect of the **Provider** or each **Contracted Processor**, in any calendar year, except for any additional audits or inspections which:

a) the **Controller** or the relevant **Controller Affiliate** undertaking an extraordinary audit if considers necessary in compliance with this **DPA**; or

b) **Controller** is required or requested to carry out by the **Applicable legislation**, a supervisory authority or any similar regulatory authority responsible for the enforcement of **Applicable legislation** in any country or territory.

13.3. The **Provider** shall, upon request also provide the **Controller** or the mandated auditor with documentation of implemented technical and organisational measures to ensure an appropriate level of security, and other information necessary to demonstrate the **Provider's** or the relevant **Provider Affiliate's** or the **Contracted Processor's** compliance with its obligations under this **DPA** and relevant **Applicable legislation**, but shall provide access to information concerning the **Provider's** or the relevant **Provider Affiliate's** or the **Contracted Processor's** other information subject to confidentiality obligations.

14. Transfer of Controller Personal Data to Countries Outside of the EEA

14.1. Transfer of **Controller Personal Data** to countries located outside of the **EEA** (if not previously mentioned hereunder) by transfer, disclosure or provision of access to data, may only occur in case of documented instructions from the **Controller** or **Controller Affiliate**.

14.2. By entering into this **DPA**, the **Controller** also grants the **Provider** the authority to enter into **Standard contractual clauses** on behalf of the **Controller** or the relevant **Controller Affiliate**, as they may be laid down by the European Commission or the applicable supervisory authority from time to time, in order to secure a valid legal basis for the transfer, disclosure or provision of access to data by **Subprocessors** outside of the EEA or international organisations. If the **Controller** is not the actual controller of the relevant **Controller Personal Data**, the **Controller** shall ensure such authorisation from the actual controller. Upon request, the **Provider** shall provide the **Controller** with a copy of such **Standard contractual clauses** or state such other valid legal basis for each transfer.

14.3. By entering into this **DPA**, the **Controller** further grants the **Provider** the authority to freely engage **Subprocessors** on behalf of the **Controller** or the relevant **Controller Affiliate** in connection with the provision of the **Service**, if such **Subprocessors** have duly undergone and achieved full self-certification in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (i.e. the new EU-USA data transfer framework as per the stated adequacy decision from the 10th of July 2023).

15. General Terms

15.1 **Governing law and jurisdiction.** Without prejudice to any applicable **Standard contractual clauses** which may have been entered into on the basis of this **DPA**:

- with respect to any disputes or claims howsoever arising under this **DPA**, including disputes regarding its existence, validity or termination or the consequences of its nullity, the parties to this **DPA** hereby agree to submit to the laws of Hungary, whereby the **Controller** or **Controller Affiliate** consents to the exclusive jurisdiction of the courts located in Hungary whereby the place of venue shall be Budapest, Hungary; and

- whereby the aforementioned laws, courts and venues shall also be used regarding all non-contractual or other obligations arising out of or in connection with this **DPA**.

15.2. **Order of precedence.** With regard to the subject matter of this **DPA** and in the event of inconsistencies between the provisions of this **DPA** and any other agreements between the parties, including the **Agreement** and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this **DPA**, the provisions of this **DPA** shall prevail.

15.3. **Liability.** Should the **Controller** suffer damages in relation to the gross negligence and/or wilful misconduct of the **Processor** in connection with this **Agreement** (except to the extent such damages had actually resulted from the gross negligence and/or wilful misconduct of the **Controller**), the **Processor** shall be liable to the **Controller** under the applicable rules for civil damages. The aforementioned shall not affect each party's liability to **Data subjects** under the **GDPR** or **Applicable legislation** or any **Standard contractual clauses** which may have been concluded in connection with this **DPA so that** such limitation of liability or liability cap would directly breach the GDPR or the **Applicable legislation**.

15.4. **Severance.** Should any provision of this **DPA** be invalid or unenforceable, then the remainder of this **DPA** shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

15.5 **Conclusion and final provisions.** No amendment to the terms and conditions of this **DPA** shall be valid unless made in writing and signed by authorised representative(s) of each party. This **DPA** may not be assigned without the prior written agreement of the other party.

15.6 This **DPA** shall be binding upon the parties and their respective successors, assigns, subsidiaries and affiliates.

15.7 This **DPA** is executed in two original copies, signed by duly authorised representatives of the parties on the day and at the place written below, each party receiving one copy thereof.

List of Appendices (2/2):

- **Appendix 1: DATA PROCESSING INSTRUCTIONS REGARDING THE PROCESSING OF CONTROLLER PERSONAL DATA IN CONNECTION WITH THE SERVICE & THE LIST OF APPROVED SUBPROCESSORS**

- **Appendix 2: LIST OF TECHNICAL AND ORGANIZATIONAL MEASURES OFFERED BY THE PROVIDER AND PROVIDER AFFILIATES FOR THE PROTECTION OF CONTROLLER PERSONAL DATA**

APPENDIX 1: DATA PROCESSING INSTRUCTIONS REGARDING THE PROCESSING OF CONTROLLER PERSONAL DATA IN CONNECTION WITH THE SERVICE & THE LIST OF APPROVED SUBPROCESSORS

This Appendix 1 includes certain details of the **Processing** of **Controller Personal Data** as required by Article 28(3) of the **GDPR** and together with the **DPA** serves as a set of data processing instructions, that have been given to the **Provider** by the **Controller** in connection with the provision of the **Service**:

Method and purpose of data collection

In order to provide the **Service** as it is set out in the **Agreement:**

a) the **Controller** may input **Controller Personal Data** directly into the **Service** himself;

b) **Controller Personal Data** may be entered into the **Service** by partners, affiliates, contractors of the **Controller** or other persons and entities that are authorised or instructed to do so by the **Controller.**

In both cases outlined above, the **Provider** is therefore instructed by the **Controller** under this **DPA** to collect, store and process the entered data, so that the **Controller** may use the **Service** in connection with relevant and consenting **End Users**, whose data is processed for the provision of the **Service**.

For the purposes of concluding the support services at the request of the **Controller** and in accordance with this **Agreement**, the data may be accessed, reviewed, backed-up, compiled, shared or otherwise processed in ways that are logically tied to the support service that is being performed at tube request of the **Controller**.

Categories of Data Subjects

The categories of **Data Subjects** whose **Personal Data** may be **Processed** under this **DPA** are defined by the **Controller** and are as follows:

- **Controller's End Users** (i.e. sport event participants as well as other individuals who offer their **Personal Data** to the **Controller** or his partners);

- other **Data Subjects** (i.e. when the **Controller** or his partners enter and use data of any other **Data Subjects** in connection with the **Service**);

whereby the **Controller** expressly warrants to the **Provider**, that he has satisfied the required lawfulness of processing based on Article 6 of the GDPR for the processing of the **Personal Data** of any and all **Data Subjects** prior to transferring them to the **Provider** or using them in any way in connection with the **Service**.

Personal Data types and the subject-matter, nature and purpose of Processing

Subject to the **Controller's** use of the **Service**, the following **Processing** may be carried out by the **Provider** or his **Subprocessors** in order to provide each sought after feature of the **Service**:

PERSONAL DATA	LEGAL GROUNDS	TYPES OF DATA & CATEGORIES OF DATA SUBJECTS	DEADLINES FOR DELETION OF PERSONAL DATA**	PURPOSES OF PERSONAL DATA PROCESSING AND TYPES OF PROCESSING*
Service data clients elect to host with	*Contract (e.g. registered user account /*	*Data (i.e. video data and other service data)*	*We store the data until account deletion (or*	*For the purposes of offering the client data*

DATASTAT d.o.o.	*concluded Data Processing Agreement)*	*that is imputed into the service and regarding which clients elect to store these data with DATASTAT d.o.o. (i.e. by choosing the non-self hosted option).*	*Until these data are deleted by the clients themselves / or the client terminates the contract).* *Note: DATASTAT d.o.o. does not store any client data if not explicitly requested to do so by the client.*	*hosting in relation to the service at the request of the client and based on the concluded Data Processing Agreement, the data may be stored, backed-up or otherwise processed in ways that are logically tied to the hosting activity.*
Service data that is processed by our employees when conducting support activities	*Contract (e.g. registered user account / concluded Data Processing Agreement)*	*Data (i.e. video data, analytical data, account related data) that is stored by users on their own servers that is accessed by our support staff.*	*The data may be stored in connection with support logs or (when requested by the client) when conducting back-ups.* *We store the data until account deletion (or until these data are deleted by the clients themselves / or the client terminates the contract).* *Note: DATASTAT d.o.o. does not store any client data if not explicitly requested to do so by the client.*	*For the purposes of concluding the support services at the request of the client and based on the concluded Data Processing Agreement, the data may be accessed, reviewed, backed-up, compiled, shared or otherwise processed in ways that are logically tied to the support service that is being performed at tube request of the client.*

*Processing special categories of personal data

Special categories of Personal Data, such as data revealing health data (namely covid test / vaccination data), may be processed under this **DPA** when the **Service** is used by the **Controller** to process such data (see the relevant section above).

The **Provider** abides by the special provisions of the **Applicable legislation** (namely the GDPR regulation) that deal with the processing and safe-keeping of **Special categories of Personal Data** and has set-up the following processes in the **Service**:

- **Special categories of Personal Data** in the **Service** are isolated and protected by internal security mechanisms and software tools that prevent possible external intrusions.

- **Special categories of Personal Data** are provided to the representative of the **Controller** or another employee of the **Controller** via a web application interface that uses a secure encrypted connection (HTTPS) that is using certificates.

- the **Service** collects audit trails on processing of these data in reviewable log files that can be made available to the **Controller**.

- Only a limited number of the **Provider**'s employees have direct access to databases that contain or may contain **Special categories of Personal Data** and may only access these data when this is strictly necessary to perform job-related tasks (recorded in the records of processing activities).

In connection to the **Special categories of Personal Data** that is processed in connection with the **Service**, the **Controller** expressly warrants to the **Provider**, that he has satisfied the required lawfulness of processing based on Article 6 of the GDPR of each and every **Data Subject** under the **Applicable Legislation**.

Timescales for the keeping of Personal Data and the duration of the Processing

The **Provider** shall keep (i.e. store in cloud storage, that is provided to him by the subprocessor that is described in this document or situationally in back-up storage, see above) **Personal Data** for as long as it is necessary to fulfill the purposes for processing and shall delete and procure the deletion of all copies of stored **Personal Data** within within 15 (fifteen) business days of the date of termination of the **Agreement** (i.e. termination by either the **Controller** or the **Provider** under point 12.1 of this **DPA**) or the termination of the registered **User** account**.**

The processing shall continue for the duration of **Controller**'s use of the **Service**, whereby most **Processing** takes place instantly after initiation by the **Controller** via the **Customer** dashboard.

Entities involved in Processing

Personal Data shall mainly be processed via automatic means by the **Service** algorithms and software systems (i.e. automatic storage of applicable data, transmission of data, making data available, combining data, etc., see above). **Provider**'s personnel shall manually process **Personal Data** upon **Controller**'s request or when performing job related tasks that require the processing of data (i.e. fulfilling requests, upkeep and monitoring of system and functions, troubleshooting, continuous development of the **Service** etc.).

List of Approved Subprocessors

The following **Subprocessors** are hereby approved by the **Controller** in relation to the provision of the **Service** under this **DPA**.
In accordance with this **DPA**, the **Provider** is instructed by the Controller to transfer **Personal Data** to the following listed **Subprocessors**:

Subprocessor	**Purpose and basis for processing**	**Country, location / protection of data**
Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States	Cloud storage via the Google Cloud service (https://cloud.google.com/terms/data-processing-terms) Analytical analysis of the use of the **Service** via implementation of the Google Analytics service (https://www.google.com/analytics/terms/dpa/dataprocessingamendment_20130906.html)	**Subprocessor entity location*:** United States of America. **Server/processing location*** – Google Cloud Storage: EEA (the Processor has selected, that the Subprocessor only stores data on servers located within the EEA) **Server/processing location*:** Users of Google Analytics, have their data scattered across randomly selected public cloud datacenters, most of which are located in the USA. **See point 14 of this **DPA** regarding the transfer of data to this USA based Subprocessor.* **Security measures:** The subprocessor's application is protected by the following security

		mechanisms and tools: dedicated security infrastructure and support, encrypted data transfer when using cloud services and encryption during transfer, DDOS protection, authentication and use of access keys, automatic encryption of stored data on server infrastructure (idle and during distribution), physical protection of servers and network equipment (Google data centres have implemented multilayered security and technical barriers to access and constant monitoring. Only approved employees with special roles can enter the data centres).

Cloudflare, Inc., 101 Townsend Street, San Francisco, United States	Security service for cloud infrastructure which improves the security, performance, and reliability of the Service (https://www.cloudflare.com/cloudflare-customer-dpa/)	**Subprocessor entity location*:** United States of America. **Server/processing location*:** EU. **See point 14 of this **DPA** regarding the transfer of data to this USA based Subprocessor.* **Security measures:** The implementation of Cloudflare's ISMS and related security risk management processes have been externally certified to the industry standard ISO/IEC 27001. Cloudflare maintains PCI DSS Level 1 compliance for which Cloudflare is audited annually by a third-party Qualified Security Assessor.

Amazon Web Services, llc., 410 Terry Avenue North Seattle, WA 98109, United States	Integration of various AWS APIs in connection with the basic functioning of the Service. (https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf)	**Subprocessor entity location*:** United States of America. **Server/processing location*:** EU. **See point 14 of this **DPA** regarding the transfer of data to this USA based Subprocessor.* **Security measures:** Security measures as per ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3) (and other measures, mentioned in the DPA).

Cloudinairy llc., 3400 Central Expressway, Suite 110, Santa Clara, CA 95051, United States	Using Cloudinairy as an end-to-end image and video management solution for image and video uploads, storage, manipulations, optimizations as well as delivery in connection with the Service. (https://cloudinary.com/gdpr/dpa)	**Subprocessor entity location*:** United States of America. **Server/processing location*:** USA. **See point 14 of this **DPA** regarding the transfer of data to this USA based Subprocessor.* **Security measures:** Cloudinary's solution is accessible via secure and authenticated HTTPS APIs, with flexible access key provisioning. Cloudinary's security features include: Automatic backup of assets to a secondary protected location. Complete asset access control. Restricted access to assets based on specific transformations, file types and referral sites via the Security page of the Console Settings. Authenticated image access with signed URLs. Access control with multiple user roles and permissions, leveraging two-factor authentication (2FA), 3rd-party service provider logins (such as Google or Github), or SSO.

GitHub Inc (GitHub), (a subsidiary of Microsoft Corp), 88 Colin P Kelly Jr St San Francisco California 94107, United States	Using the GitHub Enterprise Cloud hosting service and web interface for the Git code repository that is used for storing the code of the Service, as well as management tools for collaboration in relation to the development of the Service. (https://docs.github.com/en/sitepolicy/privacy-policies/githubprivacy-statement)	**Subprocessor entity location*:** United States of America. **Server/processing location*:** USA. **See point 14 of this **DPA** regarding the transfer of data to this USA based Subprocessor.* **Security measures:** GitHub's Information Security Management System (ISMS) has been certified against the ISO/IEC 27001:2013 standard. GitHub recognizes and supports that ISO/IEC 27001:2013 is the basis for many of our international customers' programs. GitHub offers AICPA System and Organization Controls (SOC) 1 Type 2 and SOC 2 Type 2 reports with IAASB International Standards on Assurance Engagements, ISAE 2000, and ISAE 3402 for GitHub Enterprise Cloud.

Backblaze, Inc. San Mateo, California, United States	Cloud data backup solution for certain data in the Service. (https://www.backblaze.com/company/dpa.html)	**Subprocessor entity location*:** United States of America. **Server/processing location*:** EU. **See point 14 of this **DPA** regarding the transfer of data to this USA based Subprocessor.* **Security measures:** Data Transferred via HTTPS using a strong protocol, a strong key exchange, and a strong cipher. Continuous monitor using industry standard, independent sources like SSL Labs Public/Private Keys 2048 bit public / private keys secure a symmetric AES -128 key. Data is immediately encoded for redundancy upon receipt and stored in a data centre in the account region. Data in Private Buckets can only be accessed after account authentication. Data in Backblaze B2 is protected from ransomware using object lock and third party integrations, making the data non-erasable and non-modifiable for a user-specified interval.

Mailgun Technologies, Inc., 112 E Pecan St. #1135 San Antonio Texas 78205, United States	Transactional (i.e. necessary communication) messaging service used to send, receive, and track emails in relation to the use of the Service. (https://www.mailgun.com/legal/d pa/)	**Subprocessor entity location*:** United States of America. **Server/processing location*:** EU/USA. **See point 14 of this **DPA** regarding the transfer of data to this USA based Subprocessor.* **Security measures:** 2-Factor Authentication (2FA). SAML authentication, AES-256 encryption-at-rest for all customer data. Encryption via TLS and HTTPS, Account lockdown for suspected compromise. Critical security-based log retention for 365 days. Third Party bug bounty program, Daily account data back-ups with incremental/point-in-time encrypted recovery on all primary databases. Intrusion detection systems (IDS) in place to detect unauthorized account access.
Zendesk, Inc., 989 Market St, San Francisco, CA, USA	Transactional (i.e. necessary communication) dedicated external customer support tool which allows **End users** to obtain fast responses to their questions and technical issues, whereby this service is provided to us by Zendesk Inc. (https://www.zendesk.com/company/agreements-and-terms/privacy-notice/)	**Subprocessor entity location*:** United States of America. **Server/processing location*:** EU/USA. **See point 14 of this **DPA** regarding the transfer of data to this USA based Subprocessor.* **Security measures:** Zendesk's CX products and solutions meets rigorous security, privacy, and compliance standards, including: ISO 27001:2013,ISO 27018:2014, SOC 2 Type II, EU-US & Swiss-US Privacy Shield Certification, TRUSTe Enterprise Privacy Certification

		Zendesk leverages secure components, such as FIPS-140 certified encryption solutions, to protect customer data. Portions of the Zendesk solution can be configured to meet PCI and HIPAA/HITECH Attestation standards.
Sole proprietors based in Slovenia who offer the Provider their software development services (details available upon specific request) GAVI, Mitja Železnikar s.p. Jezero 200, 1352 Preserje Reg:9064532000, VAT ID:35613491 **KTMD, ROK MAREŠ s.p.** Javor 30, 1261 LJUBLJANA-DOBRUNJE Reg:3743187000, VAT ID:SI87066785 **Tadej Puntar - informacijske rešitve s.p.** Puhova ulica 16, 1000 Ljubljana Reg:8907307000, VAT ID:13991914 **SMMX, Simon Mareš s.p.** Hlebce 13B, 4248 Lesce Reg:8597707000, VAT ID:12193330 **Ivan Širola s.p.** Presladol 67, 8280 Brestanica Reg:9329358000, VAT ID:10499571 **Matej Golob, s.p.** Pot k mlinu 22A, 2000 Maribor Reg:3168131000, VAT ID:SI33773769 **Anja Dobovšek s.p.** Teslova ulica 5, 1000 Ljubljana	*The **Provider** has engaged different sole proprietors (i.e. physical persons acting as contractors) in the Republic of Slovenia in order to contract their software development services in connection with the development and support of the **Service**, whereby the **Provider** has concluded data protection agreements with said contractors in order to uphold an equal level of obligations and security requirements related to Controller Personal Data that are no less stringent than those, which can be found in this **DPA** (concluded data protection agreements are available upon specific request).*	*The engaged sole proprietors are located and perform their subprocessing in the Republic of Slovenia.* *They perform their work from the processor's premises on the basis of a cooperation contract and a signed data processing agreement and, exceptionally (in compliance with the Processors rules on personal data protection and the Processors personal data protection policy) also from home.*

Reg:8942358000 VAT ID:39232832 **Sašo Šindič, s.p**. Puhova ulica 14,1000 Ljubljana Reg:8200033000, VAT ID:87825368		

Appendix 2: LIST OF TECHNICAL AND ORGANISATIONAL MEASURES OFFERED BY THE PROVIDER AND PROVIDER AFFILIATES FOR THE PROTECTION OF CONTROLLER PERSONAL DATA

1. PHYSICAL ACCESS CONTROL

The entrance to the common areas and the office is under supervision, with the key to the entrance of the office being held only by the head of the office, the director and any other supervising employees.

Cabinets, desks and other office furniture in which personal data carriers are kept and which are located outside the protected areas (corridors, common areas) are locked. The keys are kept by the employee who supervises the individual cabinet or desk at a designated place. Leaving keys in their locks is not allowed.

Access to the protected premises is allowed only during regular working hours, whereby access at a different time is only allowed with the permission of the responsible person (supervising employee).

Cabinets and desks containing personal data carriers are locked in protected rooms at the end of working hours or after the completion of work after working hours, while computers and other hardware are switched off and physically locked or locked through software. Leaving keys in their locks is not allowed.

Employees ensure that persons who are not employees of the company (e.g. customers, maintenance staff, business partners, etc.) do not enter the protected premises unattended, but only with the knowledge / presence of the responsible person.

2. PROTECTION OF DATA CARRIERS CONTAINING PERSONAL DATA DURING WORKING HOURS

Personal data carriers are not left in visible places (e.g. on desks) in the presence of persons who do not have the right to inspect them.

Data carriers containing sensitive or special types of personal data shall not be stored outside secure premises.

Data carriers containing personal data may be removed from the premises of the company only with the permission of the supervising employee, whereby the supervising employee shall be deemed to have given permission by engaging a certain associate in a task which includes the processing of personal data outside the protected premises.

In the premises, which are intended for performing business with external employees and/or collaborators, data carriers which contain personal data and computer displays are placed in such a way that external employees/collaborators do not have access to them.

3. HARDWARE AND SOFTWARE PROTECTION

Measures related to the organisation:

- Executed a DPIA assessment of the Service
- Engaged an external Data Protection Officer
- Determined appropriate access to databases based on job tasks and responsibilities,
- Adopted records of processing
- Adopted an internal Data Protection Security Policy
- Adopted a dedicated Data Protection Policy

Measures related to human resources:

- Dedicated Chief Security Officer
- Regular employee training
- Use of dedicated VPN system for remote work situations

Measures related to network protection:

- Separate networks for development, other office tasks and guests
- Separate network accesses based on employee credentials and tasks
- Two-factor authentication for Google Cloud storage

Measures related to hardware protection:

- Implemented specialised work stations and remote work computers
- Use of anti-virus software
- Use of employee log-in

Measures related to software protection

- Use of anti-virus software
- Use of employee log-in
- Use of separated development environments
- Use of “dummy data”
- Implemented code reviews

(A full list of protective measures and processes from the Data Protection Policy that have been put in place in connection with the Service, shall be made available upon specific request).

----------END OF DOCUMENT----------