

Medalyst Sport Innovation Kft.

PRIVACY NOTICE

ON THE RIGHTS OF DATA SUBJECTS IN RELATION TO THE PROCESSING OF THEIR PERSONAL DATA

INTRODUCTION

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: “GDPR”, “Regulation”, “General Data Protection Regulation”) requires the Data Controller to take appropriate measures to provide the data subject with all information relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and to facilitate the exercise of the data subject’s rights.

The Data Controller’s obligation to provide prior information to the data subject is also imposed by Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information. By means of the information set out below, the Data Controller fulfils this statutory obligation.

Why has this Privacy Notice been prepared?

In the course of its operations, the Data Controller processes personal data for several purposes, while respecting the rights of data subjects and complying with its statutory obligations. The Data Controller also considers it important to present to data subjects the processing of personal data of which it becomes aware in the course of its activities, together with the principal characteristics of such processing.

On what basis are the personal data of data subjects processed?

Personal data are processed only for specified purposes and on an appropriate legal basis. These purposes and legal bases are described individually in relation to each specific processing activity.

What external assistance is used in the processing of your personal data?

The Data Controller processes personal data predominantly at its own premises. However, certain operations are carried out with external assistance through data processors. The identity of the data processor may vary depending on the characteristics of each individual processing activity.

Who processes your personal data?

Chapter II of this Privacy Notice provides information to the data subject regarding the identity and contact details of the data processors engaged by the Data Controller.

What principles does the Data Controller consider important when processing your personal data?

Personal data are processed in accordance with applicable law, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016) (the GDPR).

In the course of its activities, the Data Controller processes only the personal data specified in respect of each individual processing operation, and the security of the personal data provided is safeguarded by all reasonably possible and necessary technical and organisational measures. Particular attention is paid to ensuring the confidentiality, integrity and availability of personal data.

The data subject is responsible for the accuracy and authenticity of the personal data provided. The terms used in this Privacy Notice are interpreted in accordance with the definitions set out in the Hungarian Act on the Right of Informational Self-Determination and in the GDPR.

CHAPTER I — IDENTIFICATION OF THE DATA CONTROLLER

The publisher of this Privacy Notice and the Data Controller is:

Name: Medalyst Sport Innovation Korlátolt Felelősségű Társaság (Limited Liability Company)

Registered seat: H-1071 Budapest, Damjanich utca 45., 2nd floor, door 1A, Hungary

Company registration number: 01-09-413252

Tax number: 32231867-2-42

Represented by: Tamás Béla Horovitz, Managing Director

E-mail: hello@medalyst.io

Contact: available under the “Contact” menu at <https://www.medalyst.io>

(hereinafter: “Data Controller”, “Company”)

CHAPTER II — IDENTIFICATION OF DATA PROCESSORS

Data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4(8) of the Regulation).

Engaging a data processor does not require the data subject’s prior consent, but the data subject must be informed. Accordingly, the Data Controller provides the following information:

Data processor providing accounting services

Name: Dobosi István EV. (sole proprietor)

Registered seat: H-1214 Budapest, Vénusz utca 1-3, Hungary

Tax number: 69412088-1-43

Registration number: 53146223

Data processor providing invoicing services

Company name: Billingo Technologies Zártkörűen Működő Részvénytársaság (Private Limited Company)

Registered seat: H-1133 Budapest, Árbóc utca 6, 1st floor, Hungary

Tax number: 27926309-2-41

Company registration number: 01-10-140802

Website: <https://www.bilingo.hu/>

Data processor providing online payment services

Company name: Barion Payment Zártkörűen Működő Részvénytársaság (Private Limited Company)

Registered seat: H-1117 Budapest, Irinyi József utca 4-20, 2nd floor, Hungary

Tax number: 25353192-2-43

Company registration number: 01-10-048552

Website: <https://www.barion.com/>

Other recipients

Company name: Amazon Web Services, Inc.

Registered seat: 2021 7th Ave, Seattle, WA 98121, USA

(organisation listed under the EU-US Data Privacy Framework)

Company name: MailerLite, Inc.

Registered seat: 651 N Broad St, Suite 206, Middletown, DE 19709, USA

Website: <https://www.mailerlite.com/>

(organisation listed under the EU-US Data Privacy Framework)

Company name: Google LLC

Registered seat: 1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA

Website: <https://www.google.com/>

(organisation listed under the EU-US Data Privacy Framework)

Company name: Meta Platforms, Inc.

Registered seat: 1601 Willow Rd, Menlo Park, CA 94025, USA

Website: <https://www.facebook.com/> and <https://www.instagram.com>

(organisation listed under the EU-US Data Privacy Framework)

Company name: TikTok Technology Limited

Registered seat: The Sorting Office, Ropemaker Place, Dublin 2, D02 HD23, Dublin, Ireland

Website: <https://www.tiktok.com/>

Company name: LinkedIn Corporation

Registered seat: 1000 W Maude Ave, Sunnyvale, CA 94085, USA

Website: <https://www.linkedin.com/>

(organisation listed under the EU-US Data Privacy Framework)

Where this Privacy Notice generally refers to data transfers to the Company's data processors, such reference shall also be understood to include transfers to the recipients listed above.

CHAPTER III — ENSURING THE LAWFULNESS OF DATA PROCESSING

1. Processing based on the data subject's consent

1.1. Where the Company intends to carry out processing based on consent, the data subject's consent to the processing of personal data shall be requested using the content and information set out in the data request form defined in the Company's data processing policy.

1.2. Consent shall also be deemed given where the data subject, when visiting the Company's website, ticks a box to that effect, makes the relevant technical settings when using information-society services, or makes any other statement or performs any other conduct which, in the given context, clearly indicates the data subject's consent to the intended processing of his or her personal data. Silence, pre-ticked boxes or inactivity therefore do not constitute consent.

1.3. Consent extends to all processing activities carried out for the same purpose or purposes. Where the processing serves several purposes simultaneously, consent must be given for all of them.

1.4. Where the data subject gives consent in the context of a written declaration which also concerns other matters — for example, the conclusion of a sales or service contract — the request for consent must be presented in a manner clearly distinguishable from those other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration containing the data subject's consent which infringes the Regulation shall not be binding.

1.5. The Company shall not make the conclusion or performance of a contract conditional upon consent to the processing of personal data that is not necessary for the performance of that contract.

1.6. It shall be as easy to withdraw consent as to give it. The data subject may withdraw consent at any time by sending a letter to the e-mail address provided in Chapter I.

1.7. If the data subject withdraws consent, the Data Controller may no longer process the data. Upon withdrawal of consent, the Data Controller shall ensure the deletion of the data, unless another legal basis permits processing (e.g. storage obligations or the necessity of performing a contract). Where the processing has been carried out for several purposes, the Data Controller may not use the personal data for the purpose in respect of which the data subject has withdrawn consent.

2. Processing based on compliance with a legal obligation

2.1. In the case of processing based on a legal obligation, the scope of data that may be processed, the purpose of processing, the duration of storage and the recipients shall be governed by the provisions of the underlying legislation.

2.2. Processing based on the legal ground of compliance with a legal obligation is independent of the data subject's consent, as the processing is determined by law. In such cases, the data subject must be informed before processing commences that processing is mandatory, and must be unambiguously and in detail informed of all facts relating to the processing of his or her data, in particular the purpose and legal basis of the processing, the persons authorised to carry out the processing, the duration of the processing, the fact that the Data Controller is processing the personal data on the basis of a legal obligation, and the persons who may access the data. The information must also extend to the data subject's rights in relation to the processing and to available remedies. In the case of mandatory processing, the information requirement may also be fulfilled by publishing a reference to the legal provisions containing the foregoing information.

3. Processing based on legitimate interest

3.1. A legitimate interest pursued by the Company or by a third party may constitute a legal basis for processing, provided that the interests, fundamental rights and freedoms of the data subject are not overriding. The reasonable expectations of the data subject based on his or her relationship with the controller must be taken into account; accordingly, the processing of personal data for contact or even direct marketing purposes may also be regarded as based on legitimate interest.

3.2. Processing based on legitimate interest requires a balancing-of-interests test, in which the Company always takes into account the actual circumstances and the position of the controller and the data subjects. The individual balancing-of-interests tests carried out in relation to processing in the Company's interest resulted in the following conclusion: taking into account the conditions described for each specific processing activity, the Company concluded that the processing is justified in light of the appropriate safeguards set out in this notice, since without such processing the Company would not be able to operate competitively. Accordingly, the emotional impact on data subjects and the interference with their right to privacy are considered proportionate.

4. Processing necessary to protect the vital interests of the data subject or another natural person

4.1. The protection of the vital interests of the data subject or another natural person may also constitute a legal basis for processing, given that, although the right to data protection is fundamental, it is not absolute: in matters of life and death, the right to life naturally overrides the right to the protection of personal data.

5. Processing based on contractual interest

5.1. Processing may also be based on contractual interest where it is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.

6. Facilitating the exercise of the data subject's rights

6.1. In all its processing activities, the Company is required to ensure the exercise of the data subject's rights.

CHAPTER IV — INFORMATION ON PROCESSING CARRIED OUT BY THE COMPANY

Processing of data of natural persons contracting with the Data Controller (including sole proprietors and private individuals issuing invoices)

(1) On the legal basis of performance of a contract, the Company may process — for the purposes of preparing, concluding, performing and terminating the contract, granting contractual benefits, and, in general, supporting the economic processes arising within the common sphere of interest — the following data of the natural person with whom it is in a contractual relationship: name, birth name, date of birth, mother's name, residential address, tax identification number, tax number, registration number, residential address, registered seat and place-of-business address, telephone number, e-mail address, website address, bank account number, customer number (client number, order number) and online identifier (lists of customers, suppliers, lists of loyal customers). Such processing is also lawful where it is necessary in order to take steps at the data subject's request prior to the conclusion of the contract.

(2) Duration of storage: in view of the Company's long-term business relationships, 8 years following the termination of the contract.

(3) Recipients of the personal data: those employees of the Data Controller who participate in the preparation, performance and storage of the contract may access the personal data, including the Company's executive officer, employees responsible for customer service tasks, contact persons, and the Company's data processors — in particular employees responsible for sales tasks — and other data processors. The data may also be accessed by those bodies designated by law as authorised to carry out inspections.

(4) For the purposes of postal dispatch and delivery, the personal data may be transferred to Magyar Posta (the Hungarian Postal Service) or to the courier service engaged for the purpose; for asset protection purposes, to the Data Controller's asset protection agent; and to the Data Controller's data processors.

(5) Processing is lawful where it is necessary in the context of a contract or an intention to enter into a contract (Recital 44 GDPR), or where it is necessary in order to take steps at the data subject's request prior to the conclusion of the contract (Article 6(1)(b) GDPR). Accordingly, personal data collected as part of a contractual offer may also be processed on the legal basis of performance of a contract as set out in this section. When making or receiving an offer, the Company is required to inform the offeror or the addressee of the offer accordingly.

Processing related to the issuing of invoices and the retention of accounting vouchers in connection with contracts concluded by the Data Controller

(1) Purpose of processing: issuance of invoices in accordance with Hungarian Act CXXVII of 2007 on Value Added Tax for the receipt of consideration for services, and fulfilment of the obligation to retain accounting vouchers.

(2) Data subjects: natural persons contracting with the Data Controller, or the representatives of persons contracting with the Data Controller.

(3) Scope of personal data processed: name and address of the natural person; for sole proprietors: name, registered seat and tax number; for legal persons: tax number.

(4) Legal basis: necessary for compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c) GDPR).

(5) Recipients of the personal data, or categories of recipients: the Company's data processors, in particular employees and data processors responsible for accounting and tax-related tasks, and the Hungarian National Tax and Customs Administration.

(6) Duration of storage: 8 years following the issuance of the invoice, in accordance with Section 169(2) of Hungarian Act C of 2000 on Accounting.

Processing of data of natural persons acting as signatories on behalf of legal persons contracting with the Data Controller

(1) Purpose of processing: the creation of a contract, the exercise of rights and the performance of obligations under the contract, the enforcement of any civil law claims that may arise in the course of performing the contract, and the recording and performance of obligations undertaken by the Data Controller.

(2) Data subjects: natural persons signing the contract.

(3) Scope of personal data processed: of the natural-person signatory:

- name and position (job title)
- e-mail address
- telephone number
- postal address
- specimen signature

(4) Legal basis: the legitimate interests pursued by the Data Controller, based on the balancing-of-interests test set out below (Article 6(1)(f) GDPR).

The Data Controller considers that the legal basis for processing the data of natural-person signatories complies with the legitimate-interest ground set out in Article 6(1)(f) GDPR, and that the processing does not adversely affect the interests or fundamental rights and freedoms of the data subjects in a manner that would override the Data Controller's legitimate interest (i.e. the specified interests, fundamental rights and freedoms of the data subject do not take precedence over that interest).

The legitimate interest exists	The transfer/receipt of products or the provision of services, and the documenting thereof, which is necessary in the context of performing the contract, is an interest that is not exclusive to the Data Controller but is also an interest of the contracting party as a third party, and is at the same time attributable to the performance of obligations under contract law. The Data Controller also has a significant interest in performing its contractual obligations properly and in accordance with the contract, thereby avoiding potential legal disputes. It is a legitimate business interest of the Data Controller to generate satisfaction among its contractual partners and to maintain good business relationships with them.
The processing is necessary	The processing is necessary because, without the personal data of the representative who is not a natural person but is attributable to the legal person, the legal persons and the Data Controller would be unable to establish contact with each other. In the absence of the representative's personal data, communication with contractual partners and performance of the contract would become extremely difficult, as a result of which the performance of contracts could be impeded.
The processing constitutes a proportionate restriction on the data subject	The Data Controller processes the personal data of the data subject acting as representative only to the extent necessary to achieve the legitimate business-acquisition purpose and/or to the extent necessary for establishing contact with other external bodies. The data processed do not belong to the special categories of personal data, which weighs in favour of the permissibility of the processing. The processing does not give rise to any disadvantage for the data subject acting as representative; it constitutes a proportionate restriction, as the Data Controller ensures the right to have the data subject's personal data deleted from its records upon a request to that effect or upon objection. The Data Controller restricts access to the personal data and limits such access to its own employees. It also ensures appropriate firewall and antivirus protection for the protection of the data and thereby guarantees protection of the processing that is proportionate to the risk involved.

The processing of the specimen signature is necessary for compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c) GDPR). Pursuant to Section 3:116(1) of Hungarian Act V of 2013 (Civil Code), the Data Controller is required to process the signature of the contracting partner's representative.

(5) Recipients of the personal data, or categories of recipients: those employees of the Data Controller who participate in the preparation, performance and storage of the contract may access the personal data, including the Company's executive officer, employees responsible for customer-service tasks, contact persons, and employees responsible for the Company's sales tasks, as well as those bodies designated by law as authorised to carry out inspections.

(6) Duration of storage: 8 years following the termination of the contract.

Processing of data of natural persons identified as contact persons in contracts (in the records maintained by the Data Controller) without being signatories

(1) Purpose of processing: ensuring contact in connection with the performance of the relevant contract or document, facilitating performance, and maintaining the contractual relationship.

(2) Data subjects: natural persons designated as contact persons without being signatories.

(3) Scope of personal data processed: of the natural-person contact:

- name and position (job title)
- e-mail address
- telephone number
- postal address

(4) Legal basis: the legitimate interests pursued by the Data Controller, based on the balancing-of-interests test set out below (Article 6(1)(f) GDPR).

The Data Controller considers that the legal basis for processing the contact-person data of external partners complies with the legitimate-interest ground set out in Article 6(1)(f) GDPR, and that the processing does not adversely affect the interests or fundamental rights and freedoms of the data subjects in a manner that would override the Data Controller's legitimate interest.

The legitimate interest exists	The Data Controller has a legitimate interest in ensuring contact in connection with the contracts concluded by it and in maintaining communication with the contractual partner, thereby facilitating performance of the contracts. The Data Controller also has a legitimate interest in storing the contact-person personal data of potential business partners and/or other external bodies, and in using such data in connection with future formal contact and/or the possibility of concluding contracts, which is in line with the Data Controller's activities and business-acquisition purposes.
The processing is necessary	The processing is necessary because, in the absence of contact-person data, communication with contractual partners would become extremely difficult, as a result of which the performance of contracts could be impeded.

The processing constitutes a proportionate restriction on the data subject

The Data Controller processes the personal data of the data subject acting as contact person only to the extent necessary to achieve the legitimate business-acquisition purpose and/or to the extent necessary for establishing contact with other external bodies.

The data processed do not belong to the special categories of personal data, which weighs in favour of the permissibility of the processing. The processing does not give rise to any disadvantage for the data subjects acting as contact persons; it constitutes a proportionate restriction, as the Data Controller ensures the right to have their personal data deleted from its records upon a request to that effect or upon objection.

The Data Controller restricts access to the personal data and limits such access to its own employees. It also ensures appropriate firewall and antivirus protection for the protection of the data and thereby guarantees protection of the processing that is proportionate to the risk involved.

(5) Recipients of the personal data, or categories of recipients: those employees of the Data Controller who participate in the preparation, performance and storage of the contract may access the personal data, including the Company's executive officer, employees responsible for customer-service tasks, contact persons, and employees responsible for the Company's sales tasks, as well as those bodies designated by law as authorised to carry out inspections.

(6) Duration of storage: 8 years following the termination of the contract.

Processing in connection with registration to the Medalyst browser-based web application and the iOS and Android applications

(1) Upon registration to the Data Controller's website or upon downloading the iOS or Android application, the natural person availing himself or herself of the service (hereinafter: "user") may give consent to the processing of his or her personal data by ticking the relevant box. Pre-ticking the box is prohibited.

(2) Purpose of processing: provision of the service.

(3) Data subjects: natural persons registering on the website or in the application.

(4) Scope of personal data processed: the user's name (surname, given name), e-mail address and telephone number.

(5) Legal basis: the data subject's freely given consent (Article 6(1)(a) GDPR). The consent may be withdrawn at any time. Please be informed that the withdrawal of consent does not affect the lawfulness of processing carried out prior to such withdrawal. In any request for deletion, please indicate your name and e-mail address to enable identification.

(6) The processing of personal data of children in connection with information-society services offered directly to children is lawful where the child is at least 16 years of age. For children below the age of

16, the processing of children's personal data is lawful only if and to the extent that consent has been given or authorised by the holder of parental responsibility over the child.

Verifying the child's age and verifying whether the required parental or legal-guardian consent has been provided is, in every case, the exclusive responsibility of the relevant sports association and the relevant coach. The Data Controller does not separately verify the authenticity, lawfulness or appropriateness of the consents and is under no obligation to do so. Consequently, **full responsibility for correctly establishing the age of the child and for obtaining and being able to substantiate the necessary parental or legal-guardian consent rests with the sports association and the coach, and the Data Controller excludes its liability in this regard.**

(7) Recipients of the personal data, or categories of recipients: those employees of the Data Controller who participate in the preparation, performance and storage of the contract may access the personal data, including the Company's executive officer, employees responsible for customer-service tasks, contact persons, and employees responsible for the Company's sales tasks, as well as the Company's data processors.

(8) Duration of storage: following the deletion of the registration / termination of the service or the withdrawal of the data subject's consent, access to the data shall be restricted (archived) for 90 days, exclusively for the Data Controller; the data shall be permanently deleted on the 91st day thereafter.

Linking of a parent's account with the child's profile

(1) Purpose of processing: to enable the parent or legal guardian to link, within the application, to the child's profile, and thereby to access information relating to the child and follow data relating to the child's sports activities. A further purpose of this feature is to enable the parent to identify and select his or her own child on the basis of the team roster displayed in the system.

Users acknowledge that, in order to enable parental linking, the parent will be able to see the team roster, and the selection of the child's profile will be made on the basis of that roster.

For a child who has reached the age of 16, the invitation function is available and may be used independently.

For a child below the age of 16, the invitation function is inactive by default. In such case, granting parental access and approving an invitation to a parent may take place only with the approval of a coach or administrator, in order to enable proper verification that the person requesting access is in fact the parent or legal guardian of the relevant child. Verification of parental status and the assessment and approval of access requests are within the responsibility of the coach or administrator. Prior to granting approval, the coach or administrator is required, by such reasonably available means and to the extent reasonably to be expected, to ascertain that the identity and authorisation of the requester correspond to reality, i.e. that the requester is genuinely the parent or legal guardian of the child concerned. If this cannot be properly substantiated, access must be denied.

A parent who already uses the service or application as a registered user is entitled to initiate an invitation to the other parent. However, the acceptance of the invitation and the activation of the related rights may, in this case as well, be finalised only with the prior approval of the coach.

(2) Data subjects:

- the minor or adult athlete linked to the child's profile;
- the athlete's parent or legal guardian;
- the parent initiating or accepting the invitation;
- further athletes appearing in the relevant team in the context of the display of the team roster;
- the coach and the administrator, solely in respect of the data processed in the approval and verification procedure.

(3) Scope of personal data processed:

- the child's name;
- the child's team assignment and team designation;
- the child's profile identifier or other internal system identifier;
- the name of the parent or legal guardian;
- the parent's e-mail address, user identifier and registration data;
- the fact, time and status of the invitation, and data relating to its acceptance or rejection;
- the fact of the linking between the parent and the child, and data relating to the approval of such linking;
- the fact and time of the coach's or administrator's approval and the data required for identifying the person who provided it;
- the names of the athletes appearing on the team roster.

(4) Legal basis: the processing related to the verification of parental status or legal-guardian status, the approval or rejection of access requests, and the prevention of unauthorised access, is based on the legitimate interest of the Data Controller and the relevant association. The purpose of that legitimate interest is to ensure that only persons actually authorised to do so obtain access to the child's profile, and that unauthorised persons cannot access the personal data of children.

The legal basis for the limited display of the team roster to the parent is likewise the legitimate interest of the Data Controller and the association, since the purpose of the feature is to enable the parent to identify and select his or her own child on the basis of the names of the children in the team. In doing so, only the most narrowly limited set of data necessary to achieve that purpose may be processed and displayed.

(5) Recipients of the personal data, or categories of recipients:

- authorised staff of the Data Controller;
- authorised administrators of the association;
- the coach or coaches of the relevant team;
- the approved parent or legal guardian linked to the child;

- the IT, hosting, application-operation or other technical data processors engaged by the Data Controller, to the extent necessary for the performance of their tasks.

(6) Duration of storage: personal data relating to the linking between the parent and the child's profile shall be processed for the duration of the parental access, or for as long as the child's profile remains active in the application, or for as long as the athletic relationship, team membership or user account exists.

Logging, verification and approval data generated during the invitation, approval and linking process may be retained, even after access has ceased, for as long as is necessary for the enforcement of legal claims, subsequent demonstration of authorisations, and compliance with the principle of accountability.

If the parental relationship ceases, the child leaves the team, the athletic relationship is terminated, or access is withdrawn, the linking must be terminated without undue delay, and thereafter only those data may continue to be processed which are required to be retained by law, on the basis of a legitimate interest, or for the handling of legal claims.

Team-level joining via team code and approval of the registration of minor athletes

(1) Description of processing: the application includes a "team code"-based joining feature, under which each team has a unique code. The code may be shared by the coach or the association with team members or their parents, including through closed online community platforms, messaging channels or other communication forums. By entering the team code, the user may initiate the registration or joining process or submit a request to join the relevant team.

The team code may not, in itself, result in automatic, unverified joining of the team, nor may it provide direct access to the personal data of team members. The finalisation of joining depends on the user's age and, in the case of a minor athlete, on the existence of parental approval.

For users who have reached the age of 16, joining initiated via the team code may be available independently. For athletes who have not yet reached the age of 16, the team code may serve only to initiate a registration or joining request; registration and team assignment may be finalised only after the coach or the association's administrator has verified the existence of parental or legal-guardian approval/consent.

It is the responsibility of the coach or the association to obtain parental approval/consent prior to the registration of a minor athlete, to reasonably verify the existence of such approval, and to be able to demonstrate that approval in a verifiable manner. It is the exclusive responsibility of the coach to decide whose joining is approved for the relevant team. The coach is required to ensure that approval is granted only to a person who is in fact a member of the relevant team or is otherwise entitled to join. The full verification and decision-making responsibility in this regard rests with the coach.

(2) Purpose of processing: to enable the athlete concerned, or the athlete's parent, to securely initiate joining the team using the unique team code allocated to that team, and to enable the association and the coach to manage in a verified manner the rights related to the team.

A further purpose is to ensure that, in the case of a minor athlete, registration and joining occur only with appropriate parental approval, and that access is granted only to persons actually authorised. The process is also aimed at preventing unauthorised joining, erroneous profile linking and unauthorised access.

(3) Data subjects:

- the athlete wishing to join via the team code;
- the parent or legal guardian of the athlete under the age of 16;
- the user initiating joining by entering the team code;
- the coach of the relevant team;
- the association's administrator;
- exceptionally, the other parent, where the invitation or joining is initiated by the already-registered parent.

(4) Scope of personal data:

- the athlete's name;
- the athlete's date of birth or other data necessary to verify age;
- the athlete's team and team identifier;
- the fact of the use of the team code;
- the time and status of registration, joining or team assignment;
- the name of the parent or legal guardian;
- the parent's e-mail address, user identifier or other contact data;
- the fact, time, source and data necessary for substantiating parental approval;
- the fact and time of coach/administrator approval and data required for identifying the person who provided it;
- technical log data, such as login, approval and status-change logs.

(5) Legal basis:

- For users who have reached the age of 16: the data subject's consent (Article 6(1)(a) GDPR).
- **For athletes below the age of 16, where the service qualifies as an information-society service offered directly to a child within the meaning of Article 8 GDPR, the processing of the child's personal data is lawful only if and to the extent that the holder of parental responsibility has provided the required consent or authorisation. Accordingly, the registration and team assignment of a minor athlete require that the coach or the association obtains the parental approval in advance and manages it in a verifiable manner.**

(6) Recipients, or categories of recipients:

- the authorised staff of the Data Controller;
- the authorised administrator of the relevant association;

- the coach of the relevant team;
- the approved parent or legal guardian;
- the Data Controller's technical data processors, in particular partners performing application-operation, hosting, logging or customer-service tasks, to the extent necessary for the performance of their tasks.

(7) Duration of processing: personal data relating to the joining request, the use of the team code and the approval process shall be processed until the conclusion of the joining process. After successful joining, the data relating to the athlete and the team assignment may be processed for as long as the athletic relationship, team membership or user account exists.

Processing in connection with the use of the Medalyst browser-based web application

(1) The Data Controller provides a browser-based web-application service to association administrators, the purpose of which interactive interface is to enable user associations to easily monitor the performance of athletes and staff members belonging to the association. The application also enables the administration of financial matters, the retrieval of detailed association statistics, and the monitoring of membership fees.

(2) Purpose of processing: provision of the service.

(3) Data subjects: natural persons registering in the web application.

(4) Scope of personal data processed: name of association athletes (surname, given name); date of birth; e-mail address, telephone number, address; data relating to athletic performance; registration number; the name and contact details of the legal guardian (e-mail address and telephone number); data relating to the payment of membership fees (amount of the fee, due date, fact and method of payment); and the statistical reports and analyses derivable therefrom.

(5) The data processed do not belong to the special categories of personal data. In this regard, the Data Controller specifically draws the users' attention to the fact that, in respect of the data recorded by them in the course of using the service, they are required to comply with applicable data protection rules. The Data Controller has no influence over the data recorded by users; accordingly, it assumes no liability for the lawfulness of such processing or for the handling of any data-protection irregularities relating to such data.

(6) Legal basis: the legitimate interests pursued by the Data Controller, based on the balancing-of-interests test set out below (Article 6(1)(f) GDPR).

The Data Controller considers that the legal basis for processing the data stored in the database complies with the legitimate-interest ground set out in Article 6(1)(f) GDPR, and that the processing does not adversely affect the interests or fundamental rights and freedoms of the data subjects in a manner that would override the Data Controller's legitimate interest.

The legitimate interest exists	In the context of contractual interest, and in the course of performing the contract, it is necessary to create a database that
---------------------------------------	---

	covers the persons of association athletes, the tracking of their performance, the monitoring of the association's current financial situation (membership fee amounts, receivables tracking), and the tracking of staff performance, and which is thereby suitable for significantly reducing the administrative burden on user associations. This interest is not exclusive to the Data Controller; it is also an interest of the contracting association and of the athletes within the association as third persons, given that the purpose of the database is to increase the effectiveness of the user association. The above interest is at the same time attributable to the performance of contractual obligations between the Data Controller and users. The Data Controller also has a significant interest in performing its contractual obligations properly and in accordance with the contract, thereby avoiding potential legal disputes. It is a legitimate business interest of the Data Controller to generate satisfaction among its contractual partners and to maintain good business relationships with them.
The processing is necessary	The processing is necessary because all of the above-mentioned personal data are required for tracking the performance of association members, for administering financial matters, for retrieving detailed association statistics, and for monitoring membership fees. In the absence of the above personal data, the performance of the contract would become impossible, and the contractual interest would remain unsatisfied.
The processing constitutes a proportionate restriction on the data subject	The Data Controller processes the personal data of the data subjects only to the extent necessary to achieve the legitimate business purpose. The data processed do not belong to the special categories of personal data, which weighs in favour of the permissibility of the processing. In addition, with regard to the personal data of all third persons (athletes) stored in the database, the contracting associations have obtained separate consent — that is, all athletes, or the legal guardians of minor athletes, have provided their consent to the processing of their personal data following the provision of prior information including information on the fact of profiling and on its consequences.

	The processing does not give rise to any disadvantage for the data subjects; on the contrary, the content of the database is explicitly beneficial to them, given that the database is capable of significantly reducing the administrative burden on associations and increasing their effectiveness. The Data Controller also ensures, in every case, the data subject's right to have his or her personal data deleted from the Data Controller's records upon a request to that effect or upon objection. The Data Controller restricts access to the personal data and limits such access to its own employees. It also ensures appropriate firewall and antivirus protection for the protection of the data and thereby guarantees protection of the processing that is proportionate to the risk involved.
--	--

(7) Recipients of the personal data, or categories of recipients: those employees of the Data Controller who participate in the preparation, performance and storage of the contract may access the personal data, including the Company's executive officer, employees responsible for customer-service tasks, contact persons, employees responsible for the Company's sales tasks, and the users. The Company's data processors may also have access where applicable.

(8) Duration of storage: following the deletion of the registration / termination of the service or the withdrawal of the data subject's consent, access to the data shall be restricted (archived) for 90 days, exclusively for the Data Controller; the data shall be permanently deleted on the 91st day thereafter.

Processing in connection with the use of the Medalyst iOS and Android application service (coach module)

(1) The Data Controller provides, in the form of an application available on smart devices, a service for the coaches of contracted associations. The interactive interface assists coaches in continuously tracking the development of their athletes and in communicating with athletes and with the parents of minor athletes.

(2) Purpose of processing: provision of the service.

(3) Data subjects: natural persons registering in the coach module of the application.

(4) Scope of personal data processed: name of association athletes (surname, given name); date of birth; e-mail address, telephone number, address; data relating to athletic performance; registration number; name and contact details of the legal guardian (e-mail address and telephone number); data relating to the payment of membership fees (amount of the fee, due date, fact and method of payment); and the statistical reports and analyses derivable therefrom. In addition, with respect to messages between the contracting association, coaches, athletes and legal guardians, the natural person's name (surname, given name) and the message.

The Data Controller declares that it will not use the content of communication between users for any purpose.

(5) The data processed do not belong to the special categories of personal data. In this regard, the Data Controller specifically draws users' attention to the fact that, in respect of the data recorded by them in the course of using the service, they are required to comply with applicable data protection rules. The Data Controller has no influence over the data recorded by users; accordingly, it assumes no liability for the lawfulness of such processing or for the handling of any data-protection irregularities relating to such data.

(6) Legal basis: the legitimate interests pursued by the Data Controller, based on the balancing-of-interests test set out below (Article 6(1)(f) GDPR).

The Data Controller considers that the legal basis for processing the data stored in the database complies with the legitimate-interest ground set out in Article 6(1)(f) GDPR, and that the processing does not adversely affect the interests or fundamental rights and freedoms of the data subjects in a manner that would override the Data Controller's legitimate interest.

The legitimate interest exists

In the context of contractual interest, and in the course of performing the contract, it is necessary to create a database that covers the persons of association athletes, the tracking of their performance and the monitoring of their membership-fee payment obligations, and which is thereby suitable for significantly reducing the administrative burden on user coaches and for increasing the efficiency of team management. This interest is not exclusive to the Data Controller; it is also an interest of the contracting association coach and of the athletes under his or her supervision as third persons, given that the purpose of the database is to increase the effectiveness of athlete and team management, and to facilitate smooth communication between the association, coaches, athletes and parents.

It is also in the interest of the contracting association and of the athletes within the association as third persons that the administrative burden on associations be reduced, so that, instead of operational management tasks, the focus of their operations may be on the professional activities of the sports association — i.e. competitive sport, talent development, youth development and recreational sport. Furthermore, associations operating more efficiently can also more effectively represent the interests of the athletes belonging to them vis-à-vis state bodies, sports public bodies, other sports federations, other associations and federations, and even in international sport.

The above interest is at the same time attributable to the performance of contractual obligations between the Data Controller and users.

	The Data Controller also has a significant interest in performing its contractual obligations properly and in accordance with the contract, thereby avoiding potential legal disputes. It is a legitimate business interest of the Data Controller to generate satisfaction among its contractual partners and to maintain good business relationships with them.
The processing is necessary	The processing is necessary because all of the above-mentioned personal data are required for tracking the performance and membership-fee obligations of the athletes under the coach's supervision and for retrieving detailed association statistics in respect of those matters. In the absence of the above personal data, the performance of the contract would become impossible, and the contractual interest would remain unsatisfied.
The processing constitutes a proportionate restriction on the data subject	The Data Controller processes the personal data of the data subjects only to the extent necessary to achieve the legitimate business purpose. The data processed do not belong to the special categories of personal data, which weighs in favour of the permissibility of the processing. In addition, with regard to the personal data of all third persons (athletes) stored in the database, the user coach has obtained separate consent — that is, all athletes, or the legal guardians of minor athletes, have provided their consent to the processing of their personal data following the provision of prior information including information on the fact of profiling and on its consequences. The processing does not give rise to any disadvantage for the data subjects; on the contrary, the content of the database is explicitly beneficial to them, given that the database can significantly increase the effectiveness of athlete and team management. The Data Controller also ensures, in every case, the data subject's right to have his or her personal data deleted from the Data Controller's records upon a request to that effect or upon objection. The Data Controller restricts access to the personal data and limits such access to its own employees. It also ensures appropriate firewall and antivirus protection for the protection of the data and thereby guarantees protection of the processing that is proportionate to the risk involved.

(7) Recipients of the personal data, or categories of recipients: those employees of the Data Controller who participate in the preparation, performance and storage of the contract may access the personal data, including the Company's executive officer, employees responsible for customer-service tasks, contact persons, employees responsible for the Company's sales tasks, and the users in respect of the athletes and communication data managed by them.

(8) Duration of storage: following the deletion of the registration / termination of the service or the withdrawal of the data subject's consent, access to the data shall be restricted (archived) for 90 days, exclusively for the Data Controller; the data shall be permanently deleted on the 91st day thereafter.

Processing in connection with the use of the Medalyst iOS and Android application service (athlete and parent module)

(1) The Data Controller provides, in the form of an application available on smart devices, a service for the athletes of contracted associations and, in the case of minor athletes, for their legal guardians. The interactive interface delivers only the most essential information to the athlete and the parents: information relating to events and to their performance.

The application's main functions are: the creation of events (trainings, matches, competitions, homework and other events); attendance and performance measurement; management of membership fees; communication between the association, coaches, athletes and legal guardians; and statistical summaries relating to athlete performance.

(2) Purpose of processing: provision of the service.

(3) Data subjects: natural persons registering in the athlete/parent module of the application.

(4) Scope of personal data processed: name of association athletes (surname, given name); date of birth; e-mail address, telephone number, address; data relating to athletic performance; registration number; name and contact details of the legal guardian (e-mail address and telephone number); data relating to the payment of membership fees (amount of the fee, due date, fact and method of payment); events; statistical summaries. In addition, with respect to messages between the contracting association, coaches, athletes and legal guardians, the natural person's name (surname, given name) and the message.

The Data Controller declares that it will not use the content of communication between users for any purpose.

(5) The data processed do not belong to the special categories of personal data. In this regard, the Data Controller specifically draws users' attention to the fact that, in respect of the data recorded by them in the course of using the service, they are required to comply with applicable data protection rules. The Data Controller has no influence over the data recorded by users; accordingly, it assumes no liability for the lawfulness of such processing or for the handling of any data-protection irregularities relating to such data.

(6) Legal basis: the legitimate interests pursued by the Data Controller, based on the balancing-of-interests test set out below (Article 6(1)(f) GDPR).

The Data Controller considers that the legal basis for processing the data stored in the database complies with the legitimate-interest ground set out in Article 6(1)(f) GDPR, and that the processing does not adversely affect the interests or fundamental rights and freedoms of the data subjects in a manner that would override the Data Controller's legitimate interest.

The legitimate interest exists	In the context of contractual interest, and in the course of performing the contract, it is necessary to create a database that covers the persons of association athletes, the tracking of their performance and the monitoring of their membership-fee payment obligations, and which is thereby suitable for significantly reducing the administrative burden on user athletes and, in the case of minor athletes, their legal guardians, and for increasing the efficiency of team management. This interest is not exclusive to the Data Controller; it is also an interest of the contracting athlete, given that the purpose of the database is to increase the effectiveness of athlete and team management, and to facilitate smooth communication between the association, coaches, athletes and parents. It is also in the athlete's interest that the administrative burden on associations be reduced, so that, instead of operational management tasks, the focus of their operations may be on the professional activities of the sports association — i.e. competitive sport, talent development, youth development and recreational sport. Furthermore, associations operating more efficiently can also more effectively represent the interests of the athletes belonging to them vis-à-vis state bodies, sports public bodies, other sports federations, other associations and federations, and even in international sport. The above interest is at the same time attributable to the performance of contractual obligations between the Data Controller and users. The Data Controller also has a significant interest in performing its contractual obligations properly and in accordance with the contract, thereby avoiding potential legal disputes. It is a legitimate business interest of the Data Controller to generate satisfaction among its contractual partners and to maintain good business relationships with them.
The processing is necessary	The processing is necessary because all of the above-mentioned personal data are required for tracking the athletes' performance and membership-fee obligations and for retrieving detailed association statistics in respect of those matters. In the absence of the above personal data, the performance of the contract would

	become impossible, and the contractual interest would remain unsatisfied.
The processing constitutes a proportionate restriction on the data subject	The Data Controller processes the personal data of the data subjects only to the extent necessary to achieve the legitimate business purpose. The data processed do not belong to the special categories of personal data, which weighs in favour of the permissibility of the processing. In addition, with regard to the personal data of all third persons (athletes) stored in the database, the user coach has obtained separate consent — that is, all athletes, or the legal guardians of minor athletes, have provided their consent to the processing of their personal data. The processing does not give rise to any disadvantage for the data subjects; on the contrary, the content of the database is explicitly beneficial to them, given that the database can significantly increase the effectiveness of athlete and team management. The Data Controller also ensures, in every case, the data subject's right to have his or her personal data deleted from the Data Controller's records upon a request to that effect or upon objection. The Data Controller restricts access to the personal data and limits such access to its own employees. It also ensures appropriate firewall and antivirus protection for the protection of the data and thereby guarantees protection of the processing that is proportionate to the risk involved.

(7) Recipients of the personal data, or categories of recipients: those employees of the Data Controller who participate in the preparation, performance and storage of the contract may access the personal data, including the Company's executive officer, employees responsible for customer-service tasks, contact persons, employees responsible for the Company's sales tasks, and the users in respect of their own data and, in the case of legal representation, of the minor athlete.

(8) Duration of storage: following the deletion of the registration / termination of the service or the withdrawal of the data subject's consent, access to the data shall be restricted (archived) for 90 days, exclusively for the Data Controller; the data shall be permanently deleted on the 91st day thereafter.

Processing in connection with social media (Facebook, Instagram and TikTok)

(1) The Company has only limited influence over the data processing of the operators of social-media platforms. Where the Company is able to influence and configure the relevant settings, it endeavours to facilitate, within the available options, data processing that is appropriate from a data-protection

perspective. **However, in most cases the Company is unable to influence the activities of the operator, and accordingly has no information as to which data are processed exactly.**

Facebook's privacy policy: <https://www.facebook.com/privacy/explanation/>

Instagram's privacy policy: <https://help.instagram.com/519522125107875>

TikTok's privacy policy: <https://www.tiktok.com/legal/page/eea/privacy-policy/en>

(2) The Data Controller maintains its own page on Facebook. The data subject may subscribe to the news feeds posted on the Facebook page wall by clicking the "like" link on the page. In order to contact the Data Controller via Facebook, the data subject must log in. For this, Facebook also requests, stores and processes personal data. The Data Controller has no influence over the type, scope or processing of such data, nor does it receive personal data from the Facebook operator. On the Facebook page, the Data Controller processes the personal data of followers on the basis of their voluntary consent; consent is deemed given when a person likes or follows the page, its posts, or writes a comment thereon. By requesting a service on the Data Controller's Facebook page, the data subject declares that he or she has reached the age of 16. For persons under 16, pursuant to Article 8(1) GDPR, the legal declaration containing consent to processing requires the authorisation of the legal guardian. The Data Controller is not in a position to verify the age or authorisation of the consenting person; accordingly, the data subject warrants that the data provided are accurate.

(3) Purpose of processing: providing information on current matters and on news affecting the Data Controller, advertising on social-media platforms, and the presentation and promotion of services. The Data Controller uses the Facebook page for marketing purposes, so that interested persons may become familiar with its services and may contact the Data Controller.

(4) Legal basis: the data subject's voluntary consent (in accordance with the privacy policies of Facebook, Instagram and LinkedIn).

(5) Scope of data concerned by the processing: the data subject's name; data subjects: users of the social-media platform.

(6) Duration of processing: the data subject may unsubscribe from following the Data Controller's Facebook page by clicking the "dislike" button, or may delete unwanted content using the wall settings. For the duration of the active provision of the service.

(7) Recipients: the Data Controller's employees performing customer-service and marketing-related tasks; as data processors, the Company's data processors, in particular the Company's IT service provider.

(8) The data subject acknowledges that the provision of data is not a precondition for the conclusion of a contract and that he or she is not obliged to provide personal data. A possible consequence of failure to provide data is the failure to receive information regarding current news and services affecting the Data Controller.

Processing for direct marketing purposes

(1) Unless otherwise provided by law, advertising may be communicated by way of direct contact with a natural person as the addressee of the advertising (direct marketing), in particular by way of electronic mail or another equivalent individual means of communication — with the exception set out in Hungarian Act XLVIII of 2008 — only if the addressee of the advertising has given prior, clear and express consent thereto. Pursuant to Recital 47 of the GDPR, the processing of personal data for direct marketing purposes may also be regarded as based on legitimate interest.

(2) Scope of personal data that may be processed by the Company for the purpose of contacting advertising addressees: the natural person's name, address, telephone number, e-mail address and online identifier.

(3) Purpose of processing: carrying out direct marketing activities related to the Company's business activities, i.e. the regular or periodic sending of promotional publications, newsletters and current offers in printed (postal) or electronic (e-mail) form to the contact details provided at registration.

- inviting you, by e-mail, to events organised by us that are relevant to you,
- recommending to you, by e-mail, content relevant to you,
- sending you, by e-mail, newsletters on the topics of technology, agility, training, webinars, professional presentations and events,
- contacting you with a direct offer by e-mail,
- displaying targeted advertising to you by e-mail.

The general purpose of personalised marketing messages is to increase awareness of us, as Data Controller, and of our products and services among persons interested in them. We seek to achieve this by sending you only information that is relevant to you, provided that you have given prior consent thereto.

(4) Legal basis: the data subject's voluntary consent (Article 6(1)(a) GDPR). The consent may be withdrawn at any time. Please be informed that the withdrawal of consent does not affect the lawfulness of processing carried out prior to such withdrawal. In any request for deletion, please indicate your name and e-mail address to enable identification.

(5) Recipients of the personal data, or categories of recipients: the Company's employees performing customer-service tasks; as data processors, the Company's data processors, in particular the Company's IT, marketing and newsletter service providers, and, in the case of postal delivery, employees of the postal operator.

(6) Duration of storage: until the data subject withdraws consent (until the deletion request).

Processing of data of job applicants, applications and CVs

(1) Scope of personal data that may be processed: the natural person's name, date and place of birth, mother's name, address, photograph, telephone number, e-mail address, and data relating to professional background, experience, qualifications and education.

Where, following the data subject's application, the data subject is invited to a personal interview, the Data Controller prepares a record thereof; the content of such record also qualifies as personal data.

(2) Purposes of processing:

- identifying the data subject,
- the Data Controller's assessment of the job application submitted by the data subject,
- the data subject's participation in the selection procedure,
- the selection of a data subject with appropriate skills and professional experience for the position advertised by the Data Controller,
- contacting the data subject and maintaining contact during the selection process,
- offering a subsequent job opportunity to the data subject, where the data subject is not selected for the advertised position and the data subject — following the closure of the selection procedure — has expressly consented to the retention of the application materials for this purpose.

(3) Legal basis: by submitting the application, the data subject consents (Article 6(1)(a) GDPR) to the processing of his or her personal data. (Consent is deemed given upon submission of the application), except for the possibility of offering a subsequent job opportunity. In the latter case, the applicant may declare — following the closure of the recruitment procedure — that he or she expressly consents to the further processing of the application materials for the purpose of a possible later successful recruitment.

(4) Recipients of the personal data, or categories of recipients: the Company's executive authorised to exercise employer's rights, and employees performing HR-related tasks.

(5) Duration of storage: in the case of a successful application, the Data Controller stores the data subject's personal data until the termination of the employment relationship; otherwise, the data are deleted following the assessment of the application, unless the data subject has expressly requested their retention for the purpose of further job opportunities. In such case, the Data Controller processes the application for 1 year following consent, or until the data subject's consent is withdrawn.

The Data Controller shall delete documents submitted by the data subject without undue delay upon the data subject's request. Where the data subject requests the deletion of personal data prior to the closure of the selection process, the data subject is unable to participate in the selection process.

When assessing applications, the Data Controller also reviews information that is publicly accessible on social-media platforms (Facebook, LinkedIn, Instagram, Twitter, etc.). The Data Controller handles such information solely for the purpose of becoming aware of it, and does not copy, print or record it in any manner.

Processing for the purposes of compliance with tax and accounting obligations

(1) On the legal basis of compliance with a legal obligation, and for the purpose of fulfilling tax and accounting obligations imposed by law (bookkeeping, taxation), the Company processes the legally specified data of natural persons coming into contact with it. The data processed are, in particular, the following: pursuant to Sections 169 and 202 of Hungarian Act CXXVII of 2007 on Value Added Tax: tax number, name, address, tax status; pursuant to Section 167 of Hungarian Act C of 2000 on

Accounting: name, address, the designation of the person or organisation ordering the economic operation, the person authorising the operation and the person certifying the execution of the order, and, depending on the organisation, the signature of the auditor; on inventory-movement vouchers and cash-handling vouchers, the signature of the recipient; on counter-receipts, the signature of the payer; pursuant to Hungarian Act CXVII of 1995 on Personal Income Tax: tax identification number.

(2) Processing related to the keeping of trip records and waybills (in respect of vehicles that may be used by more than one authorised person): on the legal basis of compliance with a legal obligation, and for the purposes of cost accounting, documentation, determining tax bases and accounting for fuel savings, the Company processes the legally specified data relating to the use of company vehicles and the use by employees of their own vehicles for official or business purposes (name of the driver, type and registration number of the vehicle, time and purpose of the journey, the route taken and the name of the business partner visited). The relevant law is Hungarian Act CXVII of 1995 (Personal Income Tax Act), Section 27(2)(3), Annex 6, and Annex 5(7).

(3) Duration of storage: 8 years following the termination of the legal relationship providing the legal basis.

(4) Recipients of the personal data: the Company's employees and data processors performing taxation, accounting, payroll and social-security tasks.

Processing related to payer's obligations

(1) On the legal basis of compliance with a legal obligation, and for the purpose of fulfilling tax and contribution obligations imposed by law (determination of tax, tax advance and contributions, payroll, social-security and pension administration), the Company processes the personal data prescribed by tax legislation of those data subjects — employees, their family members, persons employed under other arrangements, and other beneficiaries of payments — with whom it has a payer relationship (Section 7(31) of Hungarian Act CL of 2017 on the Rules of Taxation (Art.)). The scope of data processed is defined in Section 50 of the Rules of Taxation, including in particular: the natural person's natural-personal-identification data (including former name and title), gender, citizenship, tax identification number and social-security identification number (TAJ number). Where tax legislation attaches legal consequences thereto, the Company may process the health-related (Section 40 of the Personal Income Tax Act) and trade-union membership data (Section 47(2)(b) of the Personal Income Tax Act) of employees for the purposes of fulfilling tax and contribution obligations (payroll, social-security administration).

(2) Duration of storage: 8 years following the termination of the legal relationship providing the legal basis.

(3) Recipients of the personal data: the Company's employees and data processors performing taxation, payroll and social-security (payer) tasks.

Processing relating to documents of lasting value under the Archives Act

(1) On the legal basis of compliance with a legal obligation, the Company processes its documents qualifying as of lasting value under Hungarian Act LXVI of 1995 on Public Documents, Public Archives

and the Protection of Private Archive Materials (the “Archives Act”), for the purpose of preserving the documents of lasting value of the Company’s record-keeping for future generations in an intact and usable state. Duration of storage: until transfer to the public archive.

(2) Recipients of the personal data: the Company’s executive, the employee performing record-keeping and archiving tasks, and the staff of the public archive.

CHAPTER V — VISITOR DATA PROCESSING ON THE COMPANY’S WEBSITE — INFORMATION ON THE USE OF COOKIES

1. Visitors to the website must be informed of the use of cookies, and — with the exception of technically indispensable session cookies — their consent must be obtained.

A cookie is a small text file that is stored on the data subject’s computer or mobile device long-term data storage (HDD, SSD) until the expiry time set in the cookie, and is reactivated on subsequent visits. Its purpose is to record data relating to the visit and personal settings; however, these are data that cannot be associated with the visitor as a person. They assist in shaping a user-friendly website and enhancing the data subject’s online experience. If the data subject does not agree to the use of cookies by the data processor, the use of the website must be discontinued.

Purposes of processing:

- facilitating navigation on, and use of, the website by recording your settings and usage habits;
- improving the user experience by collecting information on how you use the website and which pages you visit or use most often, enabling us to ensure an even better user experience upon your next visit;
- collecting statistics, the analysis of which helps us understand how you use additional online services alongside the website, which we may then further develop;
- further developing and fine-tuning the website according to your needs;
- identifying potentially malicious IT operations.

Legal basis: for cookies that are essential for the proper functioning of the web interface, the Data Controller’s legitimate interest (Article 6(1)(f) GDPR). It is a legitimate interest of the Data Controller to ensure the secure operation of its website.

Where the legal basis of processing is a legitimate interest pursued by the Data Controller, you, as data subject (i.e. the person using or visiting the website), are entitled to object at any time, on grounds relating to your particular situation, to the processing of your personal data on that ground. In such cases, the Data Controller is required to substantively examine the objection submitted by the data subject and, based on the balancing of interests carried out (comparing the controller’s and the data subject’s interests), to decide on the continuation, possible restriction or cessation of the processing. The Data Controller has prepared a so-called balancing-of-interests test to substantiate its legitimate interests.

The legal basis for the processing of other cookies is the data subject's voluntary consent (Article 6(1)(a) GDPR). The consent may be withdrawn at any time. Please be informed that the withdrawal of consent does not affect the lawfulness of processing carried out prior to such withdrawal. In any request for deletion, please indicate your name and e-mail address to enable identification.

Scope of data concerned by the processing: by setting or reading cookies, we process data relating to visitors' use or browsing of the website and the related information, in accordance with the purposes of processing.

Duration of processing: we distinguish between cookies stored only for the duration of the relevant session and cookies stored for a specified, longer period. Cookies are stored only for as long as is necessary to achieve their purpose. The data subject may at any time delete the cookies stored on his or her computer or mobile phone via the browser settings.

2. Detailed information on cookies

2.1. A cookie is a piece of data that the visited website sends to the visitor's browser (in variable-name/value form) for the browser to store and subsequently allow the website to load. Cookies may have a defined validity period — they may be valid until the browser is closed, or for an unlimited period. On subsequent HTTP(S) requests, the browser also sends these data to the server. This thereby modifies the data on the user's device.

2.2. By their nature, modern website services require cookies, the function of which is to identify a user (for example, that the user has logged in to the website) and to manage the user accordingly thereafter, including on subsequent visits. The risk lies in the fact that the user is not always aware of this, and cookies may enable the website operator or another service provider whose content is embedded in the page (e.g. Facebook, Google Analytics) to track the user, thereby creating a profile of the user; in such case, the content of the cookie may be regarded as personal data.

2.3. Types of cookies

2.3.1. Technically indispensable session cookies: without these, the website simply would not function properly. They are necessary for the identification of the user — for example, for handling whether the user is logged in, what the user has placed in the cart, etc. Typically, these store a session-id, while other data are stored on the server, which is more secure. There is a security aspect: if the session cookie value is not properly generated, session-hijacking attacks become possible; for this reason, it is essential that these values be generated properly. Other terminologies refer to as "session cookies" all cookies that are deleted upon exiting the browser (a session being a browser use from launch to exit).

2.3.2. Functional cookies: these are the cookies that remember the user's choices, for example, in what form the user wishes to view the page. These cookies essentially mean the setting data stored in the cookie.

2.3.3. Performance cookies: although they have little to do with "performance" as such, this is the generally used term for cookies that collect information on the user's behaviour within the visited

website, the time spent and the clicks made. These are typically third-party applications (e.g. Google Analytics, AdWords, Yandex.ru cookies). They are suitable for profiling the visitor.

Information on Google Analytics cookies: <https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage>

Information on Google AdWords cookies: <https://support.google.com/adwords/answer/2407785>

2.4. Accepting and enabling cookies is not mandatory. You may restore your browser settings to reject all cookies, or to notify you when the system is sending a cookie. Most browsers accept cookies automatically by default, but this can generally be changed in order to prevent automatic acceptance.

Cookie settings of the most popular browsers can be configured at the following links:

- Google Chrome: <https://support.google.com/accounts/answer/61416>
- Firefox: <https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer>
- Microsoft Edge: <https://support.microsoft.com/help/4468242/microsoft-edge-browsing-data-and-privacy>
- Safari: <https://support.apple.com/en-us/HT201265>

Please be advised, however, that certain website functions or services may not function properly without cookies.

3. Information on the cookies used on the Company's website and data generated during the visit

3.1. Scope of data processed during a visit

During the use of the website, our website may record and process the following data about the visitor and the device used for browsing:

- the IP address used by the visitor,
- the type of browser,
- the operating-system characteristics of the device used for browsing (configured language),
- the time of the visit,
- the (sub)page, function or service visited,
- clicks.

These data are stored for a maximum of 90 days and may be used primarily for the investigation of security incidents.

3.2. Cookies used on the website

3.2.1. Technically indispensable session cookies

Purpose of processing: ensuring the proper functioning of the website. These cookies are necessary to enable visitors to browse the website and to use its functions and the services available through the website fully and seamlessly, including in particular remembering operations performed by the

visitor on the relevant pages, or identifying the logged-in user during a visit. The processing duration of these cookies is limited to the visitor's current visit; upon the end of the session or upon closing the browser, this type of cookie is automatically deleted from the device.

Legal basis: Section 13/A(3) of Hungarian Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services, under which a service provider may, for the purpose of providing the service, process such personal data as are technically indispensable for the provision of the service. Other conditions being equal, the service provider must select and operate the tools used during the provision of the information-society service so that personal data are processed only where this is absolutely necessary for the provision of the service and for the achievement of other purposes specified in that Act, and even then only to the necessary extent and for the necessary period.

3.2.2. Functional cookies

These remember the user's choices, for example in what form the user wishes to view the page. These cookies essentially mean the setting data stored in the cookie.

Legal basis: the visitor's consent.

Purpose of processing: increasing the effectiveness of the service, enhancing user experience, and making use of the website more convenient.

This data typically resides on the user's device; the website only accesses it and may, by means of it, recognise the visitor.

3.2.3. Performance cookies

These collect information on the user's behaviour within the visited website, the time spent and the clicks made.

Legal basis: the data subject's consent.

Purpose of processing: analysis of the website, sending of advertising offers.

CHAPTER VI — INFORMATION ON THE RIGHTS OF THE DATA SUBJECT

I. Your rights in brief

You may request the following from the Data Controller:

- information on the processing of your personal data (prior to and during the processing). Your right to information is provided by means of the preparation and publication of this Privacy Notice;
- access to your personal data (provision of your personal data by the Data Controller);
- rectification or completion of your personal data;
- erasure or restriction (blocking) of your personal data — with the exception of mandatory processing;
- you have the right to data portability;

- you may object to the processing of your personal data;
- you have the right not to be subject to a decision based solely on automated processing — including profiling — which produces legal effects concerning you or similarly significantly affects you;
- you have the right to a legal remedy.

You may submit your data-subject request to the Data Controller in writing in accordance with the Chapter on the enforcement of rights and remedies in connection with data processing. The Data Controller shall comply with your lawful request within at most 30 days, and shall notify you of this by letter sent to the contact details you have provided.

II. Your rights in detail

Right to request information (based on the controller obligations set out in Articles 13–14 GDPR)

In accordance with the Chapter on the enforcement of rights and remedies in connection with data processing, you may request information in writing from the Data Controller as to:

- which personal data of yours,
- on what legal basis,
- for what processing purpose,
- from what source,
- for how long,
- whether it engages a data processor and, if so, the name, address and processing-related activity of any such data processor,
- to whom, when and under what legal provision the Data Controller has granted access to which of your personal data, or to whom it has transferred your personal data,
- the circumstances and effects of any personal data breach and the measures taken to remedy it.

Right of access (under Article 15 GDPR)

You are entitled to obtain from the Data Controller confirmation as to whether or not personal data concerning you are being processed and, where this is the case, access to the personal data being processed; you may request this from the Data Controller in writing in accordance with the Chapter on the enforcement of rights and remedies in connection with data processing.

The Data Controller shall provide a copy of the personal data undergoing processing — unless this conflicts with another statutory obstacle. Where you have submitted the request by electronic means, the information shall be provided in a commonly used electronic form, unless you request otherwise.

Right to rectification and completion (under Article 16 GDPR)

In accordance with the Chapter on the enforcement of rights and remedies in connection with data processing, you may request the Data Controller in writing to modify a personal data item (for example, you may at any time change your e-mail address or postal address, or request the Data Controller to rectify any inaccurate personal data processed by it).

Taking into account the purposes of the processing, you have the right to request the appropriate completion of any incomplete personal data processed by the Data Controller.

Right to erasure (under Article 17 GDPR)

Erasement of personal data may, as a general rule, be requested where our processing is based on your voluntary consent — e.g. where you consented to the processing of your data (telephone number, e-mail address). In such case, your personal data will be deleted.

Your voluntary consent may be withdrawn at any time. Please be informed that the withdrawal of consent does not affect the lawfulness of processing carried out prior to such withdrawal. In any request for deletion, please indicate your name and e-mail address to enable identification.

Right to restriction of processing (blocking) (under Article 18 GDPR)

In accordance with the Chapter on the enforcement of rights and remedies in connection with data processing, you may request the Data Controller in writing to block (restrict) your personal data (by clearly marking the restricted nature of the processing and ensuring separate handling from other data).

The restriction shall last for as long as the reason specified by you renders storage of the data necessary. You may request, for example, the blocking of data where you consider that the Data Controller has processed your submission unlawfully, but it is necessary, for the purposes of administrative or court proceedings initiated by you, that the Data Controller not delete the submission.

In such case, the Data Controller shall continue to store the personal data (e.g. the relevant submission) until the authority or court contacts it, and shall delete the data thereafter.

Right to data portability (under Article 20 GDPR)

In accordance with the Chapter on the enforcement of rights and remedies in connection with data processing, you may request in writing to receive the personal data concerning you that you have provided to the Data Controller in a structured, commonly used, machine-readable format, and you have the right to transmit such data to another controller without hindrance from the Data Controller, where:

- the processing is based on consent under Article 6(1)(a) or Article 9(2)(a) GDPR, or
- on a contract under Article 6(1)(b) GDPR; and
- the processing is carried out by automated means.

Right to object (under Article 21 GDPR)

In accordance with the Chapter on the enforcement of rights and remedies in connection with data processing, you may object in writing, through the contact details provided, to the processing of your personal data based on Article 6(1)(f) GDPR (i.e. the legitimate interests pursued by the Data Controller or by a third party), including profiling based on those provisions.

In such case, the Data Controller shall no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

Automated decision-making in individual cases, including profiling (under Article 22 GDPR)

You have the right not to be subject to a decision based solely on automated processing — including profiling — which produces legal effects concerning you or similarly significantly affects you.

This right does not apply where the decision:

- is necessary for entering into, or performance of, a contract between you and the controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the rights and freedoms and legitimate interests of the data subject; or
- is based on your explicit consent.

In the cases referred to in points (a) and (c) above, the controller shall implement suitable measures to safeguard your rights, freedoms and legitimate interests, including at least your right to obtain human intervention from the controller, to express your point of view and to contest the decision.

CHAPTER VII — ENFORCEMENT OF RIGHTS AND REMEDIES IN RELATION TO DATA PROCESSING

Contacting the Data Controller

We recommend that, before initiating court or administrative proceedings, you kindly send to the Data Controller your inquiry or complaint relating to the processing of your personal data, so that we may investigate the matter and provide a satisfactory remedy, or so that we may comply with any request or claim of yours under the Chapter on the rights of data subjects — provided that it is well founded.

In the event that you exercise any of your data-processing rights under the Chapter on the rights of data subjects, request information relating to data processing, or submit an objection or complaint in relation to data processing, the Data Controller shall, without undue delay and within the period prescribed by the applicable law, investigate the matter, take action in respect of the inquiry and provide you with the relevant information. Where necessary, taking into account the complexity of the inquiry and the number of inquiries, this deadline may be extended in accordance with the statutory provisions.

Where you have submitted the inquiry by electronic means, the information shall, where possible, be provided by electronic means, unless you request otherwise. Where the Data Controller does not take

action on your inquiry without undue delay and at the latest within the period prescribed by law, it shall inform you of the reasons for not taking action and of the refusal of your request, and of the possibility of initiating court or administrative proceedings as set out below.

For the enforcement of your rights in relation to data processing, or in the event that you have any question or doubt regarding your data processed by the Data Controller, request information regarding your data, wish to submit a complaint, or wish to exercise any of your rights under the Chapter on the rights of data subjects, you may do so by submitting a data-subject request in writing, by traditional letter or by e-mail, through the Data Controller's contact details:

Medalyst Sport Innovation Korlátolt Felelősségű Társaság

Registered seat: H-1071 Budapest, Damjanich utca 45., 2nd floor, door 1A, Hungary

Telephone: +36 20 344 32 07

E-mail: hello@medalyst.io

Initiating proceedings before a supervisory authority

You have the right to lodge a complaint with a supervisory authority — in particular in the Member State of your habitual residence, place of work or place of the alleged infringement — if you consider that the processing of personal data relating to you infringes the GDPR. For the contact details of the various supervisory (data-protection) authorities within the EU, see: https://edpb.europa.eu/about-edpb/board/members_en. In Hungary, you may initiate an investigation or administrative proceedings with the Hungarian National Authority for Data Protection and Freedom of Information (NAIH; H-1055 Budapest, Falk Miksa u. 9-11.; website: <http://naih.hu>; postal address: 1363 Budapest, Pf.: 9; telephone: +36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu), on the ground that an infringement of, or imminent risk of infringement of, your rights has occurred in connection with the processing of your personal data — in particular:

- where you consider that the Data Controller restricts the exercise of your data-subject rights as set out in the Chapter on the rights of data subjects or rejects your request for the exercise of such rights (initiation of an investigation), and
- where you consider that, in processing your personal data, the Data Controller, or any data processor commissioned by it or acting upon its instructions, infringes the provisions on the processing of personal data set out in the relevant Hungarian law or in a binding legal act of the European Union (request for the conduct of administrative proceedings).

Initiating court proceedings

You may bring an action before the courts where you consider that the Data Controller is processing your personal data in breach of the provisions on the processing of personal data set out in Hungarian law or in a binding legal act of the European Union. Such proceedings may also be brought before the courts of the Member State of the data subject's habitual residence. In Hungary, such an action falls within the jurisdiction of the Regional Court (Tribunal). The data subject may, at his or her option, bring the action before the Regional Court (Tribunal) competent for the data subject's place of

residence or place of stay. For information on the jurisdiction and contact details of the courts (Regional Courts), see: <https://birosag.hu/>.

CHAPTER VIII — DATA SECURITY

The Data Controller undertakes to ensure the security of the personal data processed by it. Taking into account the state of the art and the cost of implementation, as well as the nature, scope, context and purposes of processing, and the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller takes those technical and organisational measures, and lays down those procedural rules, which ensure that the data collected, stored or processed are protected, and which prevent their destruction, unauthorised use and unauthorised alteration.

The Data Controller also undertakes to call upon any third party to which it transfers or makes available data on any legal basis to comply with the requirements of data security. The Data Controller ensures that unauthorised persons cannot access, disclose, transmit, modify or delete the data processed.

The data processed may be accessed solely by the Data Controller, its employees, the data processor(s) engaged by the Data Controller, and the recipients, in accordance with their authorisation levels. The Data Controller does not disclose the data to any third party not authorised to access them. Access to personal data by employees of the Data Controller or of a data processor takes place in accordance with their job roles, in the prescribed manner, and according to defined authorisation levels.

In order to ensure the security of IT systems, the Data Controller protects its IT systems by means of a firewall and uses anti-virus and virus-removal software to prevent external and internal data losses. The Data Controller further ensures that all incoming and outgoing communication, in any form, is appropriately monitored in order to prevent abuse.

The Data Controller and the data processor classify and treat personal data as confidential data. In order to protect data files held electronically in various records, the Data Controller ensures that the data stored in such records cannot — except for the cases specified by law — be directly linked or attributed to the data subject.

The Data Controller guarantees a level of data security commensurate with the risk, including, where appropriate:

- the pseudonymisation and encryption of personal data,
- the continuous ensuring of the confidentiality, integrity, availability and resilience of the systems and services used for processing personal data (operations and development security, protection against and detection of intrusion, prevention of unauthorised access),
- the ability to restore the availability of, and access to, personal data in a timely manner in the event of a physical or technical incident (prevention of data leakage; vulnerability and incident management),

- a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures taken to ensure the security of processing (maintenance of business continuity, protection against malicious code, secure storage, transmission and processing of data, and security training for our employees).

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

Please be advised that further detailed information on data security may be requested from the Data Controller (e-mail: hello@medalyst.io).

CHAPTER IX — TRANSFERS TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

1. On the basis of an adequacy decision (Article 45 GDPR)

Pursuant to Article 45 GDPR, the transfer of personal data to a third country or international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question, ensures an adequate level of protection corresponding to the level of EU data protection. Article 45(2) GDPR sets out the general criteria taken into account by the Commission when assessing the adequacy of the level of protection. The Commission periodically and continuously monitors the adequacy of the level of protection in those countries (in any territory thereof, in any sector or in international organisations) in respect of which it has previously adopted an adequacy decision, and, where it finds that the appropriate level of protection is no longer ensured, it shall repeal, amend or suspend its decision.

2. Transatlantic Data Privacy Framework

On 10 July 2023, the European Commission adopted an adequacy decision concerning the new EU-US Data Privacy Framework, finding that personal data can be safely transferred from the European Union to U.S. companies participating in the new framework, and that the United States ensures an adequate level of protection for personal data transferred from the EU to participating U.S. companies. A fundamental condition for joining the Transatlantic Data Privacy Framework is that the U.S. companies, as data controllers, undertake to implement data-protection measures compliant with the GDPR.

3. Transfers based on appropriate safeguards (Article 46 GDPR)

In the absence of an adequacy decision under Article 45 GDPR, a controller or processor may only transfer personal data to a third country or to an international organisation if it has provided appropriate safeguards in relation to the transfer, and on condition that enforceable data-subject rights and effective legal remedies for data subjects are available.

The Data Controller hereby informs you that, in the course of the processing activities, the personal data provided may be transferred to a third country.

CHAPTER X — RULES ON THE PROTECTION OF CHILDREN'S DATA

The personal data of children deserve specific protection, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles, and to the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility is not necessary in the context of preventive or counselling services offered directly to a child.

In the case of processing based on the data subject's consent, the processing of personal data carried out in respect of information-society services offered directly to children is lawful where the child is at least 16 years of age. Where the child is below the age of 16, processing of the child's personal data is lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

CHAPTER XI — MISCELLANEOUS

No automated decision-making takes place in the course of the processing of personal data set out in detail in this Privacy Notice.

The Data Controller reserves the right to amend this Notice unilaterally, with effect for the future. The currently effective Privacy Notice is available on the Data Controller's website. The Data Controller shall inform data subjects of amendments through its website.

Place and date: Budapest, 9 March 2026.



Medalyst Sport Innovation Kft.

Represented by: Tamás Béla Horovitz, Managing Director