Privacy Policy

1. Identification of controller

We inform you that the website https://totallsport.com/ is run by

Goal Hungary Trading and Service Limited Liability Company

Short name: Goal Hungary Kft. (Goal Hungary Ltd.)
Registration number: 03-09-125370
Tax number: 24146041-2-03
Headquarters: 11 Gazdasági vineyard, Helvécia, Hungary 6034 (Magyarország, 6034 Helvécia, Gazdasági dűlő 11.)
Postal address: 36 Küküllő Street, Helvécia 6034 Hungary (Magyarország, 6034 Helvécia, Küküllő u. 36.)
Place of business: 8-10 Dobó Istán Boulevard, Kecskemét 6000, Hungary (Magyarország, 6000 Kecskemét, Dobó István krt. 8-10.)

(Controller hereafter).

2. Legal requirements concerning processing, scope of present policy

2.1. Service of website identified by address above (website hereafter), run by Controller identified above (Controller hereafter), is supplies services from Hungary. In accordance with this, Hungarian and European law applies to service, Users during they are using services (including processing). Controller uses information about Users primarily based on these regulations:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (GDPR hereafter)
(AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet),

- Regulation CVIII of 2001 on Electronic commercial services and services related to some aspects of information society
(az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.)),
- and Regulation XLVIII of 2008 on Basic conditions and some limits of economic advertising activities (és a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény (Grt.)).

2.2. Present policy applies to processing done during the usage of the website, drawing

on services offered there, as well as fulfilling orders on the webshop.

2.3. Based on present policy, Users are: natural persons browsing the website, using the website's services and functions, and ordering products from Data Controller, who are involved in data management.

3. Processing related to information technology data collection

3.1. Controller uses ‘cookies’ to run the website and to collect technical data about the visitors of the website.

3.2. Controller represent a specific reference for visitors of the website: ‘Information about the use of cookies’

4. Processing related to receiving and answering messages

4.1. Concerned parties in processing: Users who have used the messaging surface that can be reached under ‘Contact Us' on the website or by sending an e-mail to Controller using the e-mail address(es) appeared on the website.

4.2. Legal basis of data management: User’s consent according to GDPR Article 6, Paragraph (1), Point a). In the case of the message sending form, the user gives the consent by ticking the statement that can be marked there, in the case of e-mail by sending it.

User is entitled to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing before its withdrawal. If the User withdraws their consent before replying to the message, the Controller will not continue the exchange of messages and will not answer the previously asked questions, as it must delete the data processed on the basis of the consent.

4.3. Determining the scope of data handled:

The following data of User who sent a message:
- name,
- e-mail address,
- subject of the message,
- content of the message.

4.4. Purpose of data management: to ensure exchange of messages between Controller and User.

4.5. Duration of data management: until answering a request or accomplishing User’s claim in case no contract follows the message exchange. Afterwards, Controller deletes data that is handled for these purposes. If there are more exchanges of messages, data are erased after the claim has been accomplished.

If contracting occurs during the process of exchange messages, and content of messages is important with regard to the contract, legal basis and period of processing happens based on Point 8 and Point 9 (order-related data management).

4.6. Method of data storage: in a separate data file in the information technology system of Controller.

5. Processing related to sending newsletters

5.1. Concerned parties in processing: Users who sign up for newsletters at website by ticking declaration of consent.

5.2. Legal basis of data management: User's consent based on GDPR Article 6, Paragraph (1), Point a) and User's consent subject to law regulating economic advertising activities § 6, Paragraph (1) and (2). Voluntary contribution is given by User by ticking the checkbox in front of 'declaration for subscribing' after filling up fields of subscribing for the newsletter.

User is entitled to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing before its withdrawal.

Newsletters provide useful information to users, as well as aims direct sales purposes. User can sign up for this service regardless of drawing on other services, and it is voluntary. It is based on User's decision after being informed. In case User does not take the newsletter service, they do not encounter any drawbacks when using website or any other services, it is not a criterion to use any other services at website.

5.3. Determining the scope of data handled:

for sending newsletters, User's:
- e-mail address,

to register the consent given online:
- IP-address of the device used for subscribing,
- time of subscribing.

5.4. Purpose of data management: sending newsletters to User by Controller in e-mails about Controller's services, information about the latest products/services and actualities, offers and advertisements.

5.5. Duration of data management: Controller handles information until User's cancellation of consent (User unsubscribes), or until deleting data based on User's request.

5.6. Method of data storage: in a separate data file in the information technology system of Controller.

6. Data management related to making direct sales through sending SMS and MMS messages

6.1. Concerned with data management: Users who consent to receiving SMS and MMS messages for direct sales purposes, and mark relating declaration. Furthermore, Users who give their consent to receiving SMS and MMS messages for direct sales purposes during contracting with Controller in a written form on paper or without contracting in a written form on paper.

6.2. Legal basis of data management: User's consent based on GDPR Article 6, Paragraph (1), Point a) and User's consent subject to law regulating economic advertising activities § 6, Paragraph (1) and (2). User is entitled to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing before its withdrawal.

User's voluntary contribution is given by accepting present Privacy Policy and by clicking on contribution statement of sending SMS and MMS for the purpose of direct sales or by signing the contribution statement which appears in the written contract and signing the contract itself or filling up and signing a separate paper based declaration. By doing so User declares its consent to have their data handled by the way it is specified in the data processing report and in the contract/declaration and to sending them SMS and MMS for the purpose of direct sales.

SMS and MMS messages provide Users with useful information, as well as aim at direct sales. User can sign up for this service independently from drawing on other services, and is voluntary. It is based on User's decision after being informed. In case User does not take the SMS and MMS service as part of direct sales, they do not encounter any drawbacks when using website or any other services. Controller does not give consent to direct sales purposes as a condition to use any other services at website.

6.3. Determining the scope of data handled:
- surname
- first name
- telephone number.

6.4. Purpose of data management: sending SMS and MMS messages as part of direct sales to User from Controller. They contain information about Data Manager's services, the latest products/services and actualities, offers and advertisements.

6.5. Duration of data management: Controller uses stored information to send SMS and MMS messages as part of direct sales until User's cancellation of consent (User unsubscribes), or until deleting data based on User's request.

6.6. Method of data storage: on separate data managing lists in the information technology system of Controller. Furthermore, in case User gave data that is necessary for sending SMS and MMS messages for direct sales purposes to Controller on paper, storage happens by filing paper based contracts/statements.

7. Processing related to registration

7.1. Concerned parties in processing: Users registering at website.

7.2. Legal basis of data management: based on GDPR Article 6, Paragraph (1), Point a), User's consent. Voluntary consent is given by the User by clicking on the icon depicting the schematic human figure and the button labelled "Create account", after which by filling in the registration form that appears, accepting the General Terms and Conditions and ticking the Data Management Statement, and finally clicking on the button labelled "Create".

7.3. Determining the scope of data handled:

to registrate, User's:
- surname,
- first name,
- e-mail address,

to register the consent given online:
- IP-address of the device used for subscribing,
- time of registration.

Passwords are stored with encryption codes by Controller's system as a result of which Controller cannot learn User's password.

7.4. Purpose of data management: registration on the web page and facilitating regular shopping.

7.5. Duration of data management: As for registered Users, duration of processing lasts until Users request for data deletion. Processing may finish when User deletes their registration or when Controller deletes User's registration. User may delete their registration anytime, or can ask Controller to do so. Such incoming requests are handled and accomplished immediately, but within no more than 10 working days after the request arrives.

7.6. Method of data storage: in a separate data file in the information technology system of Controller.

8. Data processing related to Users' contracting

8.1. Concerned parties in processing: natural person (consumer) Users who place orders on the website.

8.2. Legal basis of data processing: based on GDPR Article 6, Paragraph (1), Point b), according to which processing is necessary to accomplishing contracts where User is one of the parties.

8.3. Determining the scope of data handled: Processing involves personal data and contacts.

Users who are making an order:
- surname,
- first name,
- billing address,
- address of delivery,
- telephone number,
- e-mail address,
- indication of product(s) ordered,
- price of product(s) ordered,
- delivery method,
- payment method,
- other information User might have provided in order to accomplish order,
- time of order,
- time of payment.

8.4. Purpose of data processing: to make and fulfil contracts realized through orders.

8.5. Duration of data processing: Controller processes the data on the basis of its legitimate economic interest until the expiration of the limitation period for claims arising from the contractual legal relationship - which is usually 5 years from the date the claim became due. Any interruption of the statute of limitations extends the duration of data processing until the new date of the statute of limitations.

During delivery - through which order is fulfilled - processing of necessary data (Buyer's name, address of delivery, telephone number, data related to product delivery and payment of the price in case of cash on delivery) lasts until the delivery is accomplished. When Controller forwards personal information to delivery company exclusively necessary for delivery, uses processing limitation, so data forwarded can be used only to a limited extent and time for the purpose of data management.

However, it is in the legitimate interest of the company performing the delivery to further preserve the above data or part of it in the event of possible complaints, reclamations or civil disputes. However, delivery company does this as independent Controller, User may read about this in specific service provider's privacy policy. User can get more information about such service providers in chapter "Using a Processor" of present policy, where their websites containing their privacy policy is indicated as well.

The Controller handles the accounting documents issued in connection with the order for the time necessary to fulfil the document retention obligation, according to Chapter 11.

8.6. Method of data storage: in a separate data file in the information technology system of Controller, and on accounting documents that correspond to related laws about keeping bills for certain periods of time.

8.7. Consequences of failure to provide data: the provision of the data necessary to fulfil the order by the User placing the order is a prerequisite for entering into a contract. If

the User wishes to place an order, he/she must provide the above listed data. If data is not provided, the Controller cannot fulfil the order.

9. Data processing related to ordering on behalf of an organization in the case of a natural person acting on behalf of an organization

9.1. Concerned parties in processing: natural person Users (or 'Representor') on behalf of the organization that place orders on the webpage.

9.2. Legal basis of data management: According to GDPR Article 6, Paragraph (1), Point f), data management is the legitimate interest of the organization ('Partner Organization' afterwards) which is represented by User.

Contracting with Controller in order to order products is the legitimate interest of the Partner Organization. This can be maintained through using a natural person Representor.

Controller processes Representor's data exclusively in connection with administration and fulfilment of contract in connection with the organization he/she represents, to the extant and time necessary to it and as for the circle of data it is restricted solely to necessary data.

Placing the order and necessary information exchange for fulfilling the contract will not be possible without handling the Representor person's data ergo data management is unavoidable for contracting.

A separate documentation is made about considering interests. Representor can ask information about how to reach it from Controller.

9.3. Determining the scope of data handled:

The representing person's:
- surname,
- first name,
- e-mail address,
- telephone number,

The represented company's:
- type,
- name,
- postal address,
- billing address,
- VAT number, VAT registration number.

Furthermore, data of purchasing:
- indication of product(s) ordered,
- price of product(s),

- delivery method,
- payment method,
- other information User might have provided in order to accomplish order,
- time of order,
- time of payment.

9.4. Source of data: normally the User. In case it is not the Representor itself, who gives data but someone else from the Partner Organization, the source of data is the Partner Organization. Controller takes over Representor's data in the legal interest of the Partner Organization. It is the Partner Organization's duty to notify Representor about data processing: handing over Representor's data to Controller.

9.5. Purpose of data management: to sign and fulfil a contract resulting from an order for Users who represent companies.

9.6. Duration of data management: Controller processes the data on the basis of its legitimate economic interest until the expiration of the limitation period for claims arising from the contractual legal relationship - which is usually 5 years from the date the claim became due. Any interruption of the statute of limitations extends the duration of data processing until the new date of the statute of limitations.

During delivery - through which order is fulfilled - processing of necessary data (Buyer's name, address of delivery, telephone number, data related to product delivery and payment of the price in case of cash on delivery) lasts until the delivery is accomplished. When Controller forwards personal information to delivery company exclusively necessary for delivery, uses processing limitation, so data forwarded can be used only to a limited extent and time for the purpose of data management.

However, it is in the legitimate interest of the company performing the delivery to further preserve the above data or part of it in the event of possible complaints, reclamations or civil disputes. However, delivery company does this as independent Controller, User may read about this in specific service provider's privacy policy. User can get more information about such service providers in chapter "Using a Processor" of present policy, where their websites containing their privacy policy is indicated as well.

The Controller handles the accounting documents issued in connection with the order for the time necessary to fulfil the document retention obligation, according to Chapter 11.

9.7. Method of data storage: in a separate data file in the information technology system of Controller, and on accounting documents that correspond to related laws about keeping bills for certain periods of time

9.8. Consequences of failure to provide data: the provision of the data necessary to fulfil the order by the User placing the order is a prerequisite for entering into a contract. If the User wishes to place an order, he/she must provide the above listed data. If data is not provided, the Controller cannot fulfil the order.

10. Data management concerning refunds

10.1. In case of money refund when User paid by credit card or by any other online payment ways through paying services User can get back the paid amount of money through the given means of payment or paying service that was originally used. In case User paid requests a refund by bank transfer then Controller pays back the amount of money by bank transfer.

10.2. Concerned parties in processing: User who placed the order and affected by money refund.

10.3. Legal basis of data management: according to GDPR Article 6 paragraph 1, point (c) in compliance with legal obligation of the Controller.

10.4. Determining the scope of data handled:
- order ID,
- the sum to be refunded,
- legal title of refund,
- User’s name,
- bank account number in case User requests the money back by bank transfer.

10.5. Purpose of data processing: fulfilment of obligations related to the exercise of the warranty right and the right of withdrawal.

10.6. Duration of data management: The Data Controller processes the data on the basis of its legitimate economic interest until the expiry of the statute of limitations for refund-related claims - which is, in general, 5 years from when the claim became due. Any interruption of the statute of limitations extends the duration of data processing until the new date of the statute of limitations.

In connection with the refund, the data controller processes the accounting receipts issued in connection with the order for the time necessary to fulfil the obligation to preserve the receipts prescribed by the Accounting Act, in accordance with Chapter 11.

10.7. Method of data storage: in a separate data file in the information technology system of Controller, and the data required for regular accounting in order to fulfil the document retention obligation prescribed by the Act on Accounting on accounting documents.

11. Data processing related to the preservation of accounting document

11.1. Concerned parties in processing: Users placing orders on the website.

11.2. Legal basis of data management: according to GDPR Article 6 paragraph 1, point (c) in compliance with legal obligation of the Processor.

11.3. Determining the scope of data handled:

The User:

- surname,
- first name,
- billing address,
- address of delivery,
- telephone number,
- e-mail address,
- indication of product(s) ordered,
- price of product(s) ordered,
- delivery method,
- payment method,
- other information User might have provided in order to accomplish order,
- time of order,
- time of payment.

11.4. Purpose of data processing: to issue an invoice and to fulfil the obligations regarding the preservation of accounting documents.

11.5. Duration of data processing: Processor handles information mentioned above until it is prescribed by the Act on Accounting about keeping certificates. According to the Act on Accounting, this period is at least 8 years after making out an receipt, after passing this deadline, Processor deletes data within one year. This scope primarily includes the data on the invoices (Buyer's name, address, data relating to the ordered product and the payment of its price), and as part of the contractual documentation, the additional data included in the orders and confirmations also fall under the concept of accounting documents.

11.6. Method of data storage: On separate data line within the Processor's information technology system, and on accounting documents that correspond to related laws about keeping bills for certain periods of time.

12. Data processing related to consumer complaints

12.1. Concerned parties in processing: Users reporting consumer complaints.

12.2. Legal basis of data management: according to GDPR Article 6 paragraph 1, point (c) in compliance with legal obligation of the Controller; concerning the Data Processor in relation to the handling of complaints, fulfilment of legal obligations.

12.3. Determining the scope of data handled:
The complaining User:
- surname,
- first name,
- address,
- place, time and way of proposing the complaint,
- a detailed description of his/her complaint,
- presented by the User in the complaint; all personal data that the User brings to the attention of the Data Controller in connection with his/her complaint,

- personal data contained in documents, files and other evidence that may be presented by the User,
- the place and time of taking the record of the complaint,
- in the case of a written complaint, the User's signature,
- in the case of a complaint sent by e-mail, the e-mail address of the User,
- in the case of a verbal complaint communicated by telephone or using other electronic communication services, the unique identification number of the complaint and the User's telephone number,
- possibly the identifier of the order or other transaction affected by the complaint and the information regarding its fulfilment.

Telephone calls are not recorded by the Data Processor.

12.4. Source of data: User provides the data to Data Processor in his/her complaint. The investigation of the complaint may also require the processing of data related to the User's previous order placed with the Data Controller. The Data Processor does not obtain the User's data from other (external) sources.

12.5. Purpose of data processing: investigating and responding to the complaint submitted by the User; fulfilment of legal obligations related to the investigation of the complaint by the Data Controller.

The purpose of processing the User's personal identification data is to identify the User, which is necessary to investigate and respond to their complaint.

Information containing personal data presented in the User's complaint, as well as the data of the previous order possibly involved in the complaint, will be used for the substantive investigation and response to the complaint, if they are necessary for all of this

The User's name and address will be used to address the mail, in case the record of the complaint or the response to the complaint is sent in writing by the Data Processor by post.

The User's name and e-mail address may be used to communicate via electronic mail (if this is necessary to investigate the complaint) and to respond to User’s complaint by e-mail.

12.6. Duration of data management: According to Article 17/A of the Consumer Protection Act, Data Processor shall keep the record of the complaint, or, in the case of a written complaint, the submitted document and the response to the complaint for three years, after which it shall be destroyed.

If the submitted claim is not considered a complaint, the Data Processor will delete the data one month after the end of the communication related to the claim.

If the notification is not considered a complaint, but refers to a specific transaction related to the performance of the Data Processor and has relevant content to that, in that case, the Data Processor will process the claims arising from the contractual relationship

until the expiry of the statute of limitations - which is usually 5 years from the date the claim became due - after which Data Processor will delete the data.

12.7. Method of data storage: In a separate data file in the IT system of the Data Processor, possibly on paper depending on the method of submission, in the record of the complaint, as well as in the document containing the response to the complaint.

13. Data processing related to reporting objections

13.1. Concerned parties in processing: Users reporting claims for the enforcement of warranty rights.

13.2. Legal basis of data management: according to GDPR Article 6 paragraph 1, point (c) in compliance with legal obligation of the Controller.

13.3. Determining the scope of data handled:

The User’s:
- surname,
- first name,
- postal address,
- place, time and way of reporting the objection,
- detailed description of the objection,
- those presented by the User in the objection; all personal data that the User brings to the attention of the Data Controller in connection with his/her objection,
- method of settling objections,
- content of a response to an objection,
- in case of refusal to settle the objection, the reason for it,
- the conclusions that can be drawn based on the documents, documents and other evidence presented or handed over by the User, as well as the personal data contained in them,
- in case of an objection sent by e-mail, the e-mail address of the User,
- in the case of a verbal objection communicated by telephone or using other electronic communication services, the unique identification number of the objection notification and the User's telephone number,
- the identifier of the order or other transaction affected by the objection.

Telephone calls are not recorded by the Controller.

13.4. Source of data: the data is provided by the User to the Data Controller. The Data Controller does not obtain the User's data from other sources.

13.5. Purpose of data processing: investigation and response to the warranty-related complaint submitted by the User.

13.6. Duration of data management: the data processed during objection management is processed by the Controller until the expiry of the general statute of limitations

applicable to civil claims, which in the basic case is 5 years from the end of handling the objection.

Interruption of the statute of limitations extends the duration of data management until the new date of statute of limitations.

13.7. Method of data storage: in a separate data file in the information technology system of Controller, as well as the record of the objection notification on a paper basis.

14. Forwarding data

14.1. Scope of concerned: Users choosing online payment after shopping at website, regardless of using other services.

14.2. Addressee of data forwarding:

PayPal (Europe) S.a.r.l. et Cie, S.C.A. (PayPal)

Short name: PayPal S.a.r.l.
Corporate registration number: B118349
Tax number: LU 22046007
Premises: 22-24, Boulevard Royal, 2449 Luxembourg, Luxembourg
Postal address: 22-24, Boulevard Royal, 2449 Luxembourg, Luxembourg
Telephone: -
E-mail: dpo@paypal.com
Website: https://www.paypal.com

as service provider company of online payment service available at Controller's website

Furthermore,

OTP Mobile Services Ltd. (SimplePay)
(OTP Mobil Szolgáltató Kft.)

Corporate registration number: 01-09-174466
Tax number: 24386106-2-42
Premises: 17-19, Hungária Boulevard Budapest 1143 Hungary (Magyarország, 1143 Budapest, Hungária körút 17-19.)
Postal address: 17-19, Hungária Boulevard Budapest 1143 Hungary (Magyarország, 1143 Budapest, Hungária körút 17-19.)
Telephone: +36 1 1/20/30/70 3-666-611
E-mail: ugyfelszolgalat@simple.hu
Website: https://www.simplepay.hu/

as service provider company of online payment service available at Controller's website.

14.3. Legal basis of data forwarding: User's legitimate interest based on GDPR Article 6, Paragraph (1), Point a). Recipient is obliged to run a fraud prevention and scout system

in connection with offering payment services and has the right to handle personal data that is necessary for these. Recipient has developed its system regarding to legal obligations, for its operation data forwarding by Controller is necessary. Accordingly to this it is Recipient's legitimate interest to run a fraud prevention and scout system to meet its legal obligations. Recipient falls under the following provisions:
- Act CCXXXVII of 2013 165. § (5) Paragraph on Credit Institutions and Financial Enterprises (a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 165. § (5) bekezdése),
- Act CCXXXV of 2013 92/A. § (3) Paragraph Point f) on some payment services (az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 92/A. § (3) bekezdés f) pontja),
- Act LXXXV of 2009 14. § (1) Paragraph Point v) on providing payment services (a pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény 14. § (1) bekezdés v) pontja).

Fraud prevention and providing proper operation of online services are both Controller's and Recipient's legitimate interest. Both organisations' main source of revenue connects to proper operation of payment services. Nevertheless these are User's interests as well, in particular to avoid abuse of bank card data.

Data forwarding allows preventing and detecting frauds and troubleshooting of possible stumbling block that might appears during the process of payment.

Forwarded data comes from User's data handled during booking/ordering and these data are forwarded through electronic channels which ensure encrypted data traffic solely for Recipient and only after payment is done and which are not used for any other purposes by Recipient. Therefore, data forwarding puts no significant risk on User , it has no other visible effect on them.

Forwarding data is necessary for reaching goals described here and is suitable for making payment services safer.

In view of the above and taking the built in guarantee operations into account, forwarding does not mean unreasonable degree encroachment into Users' personal lives, therefore data forwarding is a necessary and proportional data processing operation.

A separate documentation is made about the consideration of interests whose details can be required by User from Controller.

14.4. Scope of data forwarding:

- surname,
- first name,
- e-mail address,
- address,
- Unique identifier of the transaction.

Bank card data given during payment is directly provided for payment service provider, so Controller does not gain access to them.

14.5. Purpose of forwarding data: Operating and managing online payment service appropriately, confirmation of transactions, operating fraud-monitoring to protect users' interests. This is a system to reveal frauds related to online payment, supporting the control of bank transactions – and providing help through customer support service.

14.6. Data security: data security is based on the separation of data. Data Controller receives information about the order from the User, and the payment service provider only receives the bank card data required for the payment transaction on the payment page with 128-bit SSL encryption. To pay by bank card, your internet browser must support SSL encryption. SSL stands for Secure Sockets Layer accepted encryption method. The browser used by the User uses SSL to encrypt the bank card data before sending it, so that it reaches the payment service provider in coded form and cannot be interpreted by unauthorized persons.

14.7. Controller does not forward information to third parties for business or marketing purposes.

14.8. Controller forwards information only to official bodies in accordance with legal requirements beyond the above mentioned cases.

15. Using data processing

Controller draws on the following businesses to process data.

15.1. Storage space service provider

15.1.1. Data subjects involved in the processing: Users visiting website, regardless of using services.

15.1.2. Controller uses

WEB HOSTING Limited Liability Company
(WEB HOSTING Korlátolt Felelősségű Társaság)

Short name: WEB HOSTING Kft. (WEB HOSTING Ltd.)
Corporate registration number: 18-09-113921
Tax number: 24954013-2-18
Headquarters: 2/14 Semmelweis Ignác Street Szombathely 9700, Hungary (9700 Szombathely, Semmelweis Ignác utca 2. 14.)
Postal address: 2/14 Semmelweis Ignác Street Szombathely 9700, Hungary (9700 Szombathely, Semmelweis Ignác utca 2. 14.)
Telephone: +36 94 514 333
E-mail: info@webhostingkft.hu
Website: https://webhostingkft.hu/

as website storage place provider (Data Processor hereafter).

15.1.3. Defining the scope of data involved in data processing: this potentially relates to all information mentioned in present policy, the specific data circle is defined by functions used by User according to the above chapters of specific data managements.

15.1.4. Purpose of using data processor: To ensure functioning of website in an information technological way by using electronical host and software that is necessary for it.

15.1.5. Method of data processing: it is done electronically; processing data exclusively means to provide storage space and functionality of the software that is necessary for the operation of website in an information technological way.

15.2. Data processing in relation with sending newsletters

15.2.1. Data subjects involved in the processing: Users subscribing to newsletters, regardless of whether they use any other services.

15.2.2. Controller uses services of

E.N.S. IT and System Integration Private Limited Company

E.N.S. Informatikai és Rendszerintegrációs Zártkörűen Működő Részvénytársaság (Webgalamb)

Short name: E.N.S. Zrt.
Corporate registration number: 01-10-046975
Tax number: 14032868-2-42
Headquarters: 2nd Floor 2nd Building 10 Fehér Road Budapest 1106 Hungary (Magyarország, 1106 Budapest, Fehér út 10. 2. ép. 2. em.)
Establishment: 1 Dr Dunay Alajos Street Békésszentandrás 5561 Hungary (Magyarország, 5561 Békésszentandrás, Dr. Dunay Alajos utca 1.)
Postal address: 2nd Floor 2nd Building 10 Fehér Road Budapest 1106 Hungary (Magyarország, 1106 Budapest, Fehér út 10. 2. ép. 2. em.)
Telephone: +36 30 555 1100
E-mail: info@ens.hu

as company that has developed and operates the newsletter sending software that is used by Controller (Data Processor hereafter).

15.2.3. Defining the scope of data involved in data processing: User’s e-mail address who subscribed for receiving newsletters.

15.2.4. Purpose of using data processors: to provide information technological conditions for sending newsletters by Controller, in processing apparent through technical operations necessary for operating the software safely.

15.2.5. Method of data processing: Processing data exclusively refers to technical operations to manage software about sending newsletters in an information technological

way.

15.3. Data processing related to delivery company

15.3.1. Data subjects involved in the processing: Users placing an order and asking for delivery.

15.3.2. Controller uses services of

GLS General Logistics Systems Hungary Csomag-Logisztikai Korlátolt Felelősségű Társaság
(GLS General Logistics Systems Hungary Ltd.)

Short name: GLS General Logistics Systems Hungary Kft.
Corporate registration number: 13-09-111755
Tax number: 12369410-2-44
Headquarters: 2, GLS Európa Street, Alsónémedi 2351, Hungary (2351 Alsónémedi, GLS Európa u. 2.)
Postal address: 2, GLS Európa Street, Alsónémedi 2351, Hungary (2351 Alsónémedi, GLS Európa u. 2.)
Telephone: +36 29 886 670
E-mail: info@gls-hungary.com
Website: https://gls-group.eu/

as **delivery company** that delivers ordered products(Processor hereafter), as well as a delivery point and parcel locker provider.

15.3.3. Defining the scope of data involved in data processing: in order to fulfil the contractual obligation (performing delivery) that comes from User’s order, data management affects the following data:
- surname
- first name
- e-mail address
- telephone number
- address of delivery.

15.3.4. Purpose of using data processor: In order to fulfil the contract made when User places an order, the goal is to deliver the ordered product to an address indicated by User, checking delivery address and time if necessary on the phone.

15.3.5. Method of data processing: it affects only those data management operations that are necessary to fulfil delivering and handing over the product.

16. Data protection, data safety

16.1. Controller assures the safety of data and through technical and organizational actions, as well as internal rules of procedure ensures that laws and other data and secret protection rules are kept. Controller protects data especially against illegal access, change, forwarding, making public, deletion or effacement of data, moreover, it protects against accidental effacement and damage, as well as inaccessibility of data as a result of change in applied technology.

16.2. Data related to measuring number of visitors of the website and habits describing use of website are handled in Controller's information technological system in a way that prevents Controller to link data to anyone, right from the beginning.

16.3. Processing takes place to reach articulated and legal goals described in present policy to a necessary and proportional degree, based on relevant laws and recommendations, keeping appropriate safety measures.

16.4. In order to achieve these, Controller uses "https" protocol to reach the website, through which web communication can be encrypted and individually identifiable. Controller stores information in encrypted data stocks on separate lists insulated from each other based on processing goals to which certain Controller employees – performing tasks indicated in present policy – have access to, who have to protect data and it is their responsibility to handle this policy and relevant laws in an appropriate manner.

16.5. The Controller concludes a data processing contract with the data processors it uses with mandatory content to comply with the relevant legislation and to guarantee an adequate level of data security.

16.6. Passwords are stored with encryption by Controller's system as a result of which Controller cannot learn User's password.

17. User's rights concerning data processing

17.1. Right to information

17.1.1. By reading this data processing information, the User can find out about data management at any time. Verbal information can also be provided at the User's request, provided that the User's identity has been verified in another way. The User may request information during and after being involved in data management. The information covers all essential details of data processing, as well as the method of exercising the User's rights. Upon the User's request, the Controller will also inform the User of the measures taken based on the User's requests - or of the reason for their failure, indicating the forums available for presenting the complaint.

17.1.2. Providing information is free of charge. If User's request is obviously unfounded, or – especially for its repeated nature – exaggerated, Controller
a) might charge a reasonable price, or
b) might deny taking actions based on request,
considering data requested, or administrative costs of measures to be taken to fulfil

request.

17.1.3. As soon as possible from the submission of the request (without undue delay), but within one month at the latest, the Controller shall provide the access described above.

17.2. Right to access

17.2.1. The User has the right to access the data processed about him. In the event of such a request, the Controller shall inform the User of whether data processing is in progress with regard to the User's personal data, as well as of all relevant circumstances related to the specific data processing.

17.2.2. Pursuant to the right of access, the User may request a copy of his personal data managed by Controller, which the Controller will provide free of charge for the first time. For additional copies, Controller calculates a reasonable fee based on administrative costs.

17.2.3. The copy is provided by Controller in a widely used electronic format, unless the User requests otherwise.

17.2.4. As soon as possible from the submission of the request (without undue delay), but within one month at the latest, the Controller shall provide the access in accordance with the above.

17.3. Right to correction

17.3.1. The User has the right to request that the Controller correct inaccurate personal data relating to him/her without undue delay.

17.3.2. Considering the goal of processing, User has the right to ask for completing their missing personal data – for example through an additional declaration.

17.3.3. At the user's request, Controller shall correct without undue delay or, in justified cases, supplement inaccurate personal data relating to him/her.

17.4. Right to cancellation

17.4.1. The User has the right to request that Controller delete personal data concerning him/her without undue delay, and the Controller is obliged to delete personal data concerning the User without undue delay if one of the following reasons exists:

a) personal data is no longer needed for reasons they were recorded, or were handled differently;

b) User withdraws their consent to processing, and there are no other legal bases for it (of the data processing that is the subject of this information, it only exists in the case of data processing performed on the basis of legitimate interest, presented in the following

chapters:
3. Technical data processing related to ensuring the operation of information technology services based on consent;
4. Processing related to receiving and answering messages;
5. Processing related to sending newsletters;
6. Data management related to making direct sales through sending SMS and MMS messages;
7. Processing related to registration;

c) User objects to processing and there are no prior rightful reasons for processing (of the data processing that is the subject of this information, it only exists in the case of data processing performed on the basis of legitimate interest, presented in the following chapters:
3. Technical data processing related to ensuring the operation of information technology services based on legitimate interest;
9. Data processing related to ordering on behalf of an organization in the case of a natural person acting on behalf of an organization;
14. Data transmission in connection with online payment);

d) personal data was processed illegally;

e) personal data must be deleted to fulfil legal obligations claimed by European Union or member state laws.

17.4.2. The Controller is not obliged to delete the data necessary for the submission, validation and protection of legal claims, even in the event of a request from the User, nor those whose treatment is necessary to protect the vital interests of the User or other natural person, or to fulfil an obligation under EU or member state law applicable to the Controller. By default, however, after the retention period has expired, the Controller deletes the data without a request.

17.5. Right to limitation of processing

17.5.1. At the User's request, the Data Manager limits data processing if one of the following is met:
a) User disputes accuracy of personal data, in this case limitation exceeds for the period that enables Controller to check the accuracy of personal data;
b) processing is illegal, and User objects against deleting their data and asks for limitation of use;
c) Controller does not need personal data for processing, however, concerned party lays claim to them in order to propose, realize or protect legal demands; or
d) User objected to data management; in this case, the restriction applies to the period until it is determined whether the legitimate interests of the Controller take precedence over the legitimate interests of the User (of the data processing that is the subject of this information, it only exists in the case of data processing performed on the basis of legitimate interest, presented in the following chapters:
3. Technical data processing related to ensuring the operation of information technology

services based on legitimate interest;
9. Data processing related to ordering on behalf of an organization in the case of a natural person acting on behalf of an organization;
14. Data transmission in connection with online payment).

17.5.2. If data management is subject to restrictions, such personal data, with the exception of storage, will only be processed by the Controller with the consent of the User, or to submit, enforce or defend legal claims, or to protect the rights of other natural or legal persons, or in the important public interest of the European Union or a member state.

17.5.3. The Controller informs the User, who contested the accuracy of the personal data, and the data processing was restricted based on this, of the lifting of the data processing restriction in advance.

17.6. Notification obligation related to the correction or deletion of personal data, or the limitation of data processing

Controller informs the User and all those recipients that are provided with information about the correction, limitation and deletion. Notification might be neglected if it seems to be impossible, or requires unreasonable efforts. Controller informs User on demand about these addressees.

17.7. Right to portability of data

17.7.1. User has the right to get personal data about themselves in an articulate, widely used format, readable on devices, furthermore, has the right to forward these pieces of information to another Controller without the obstruction of Controller that has User's data according to User's consent, if:
a) processing is based on User's consent or contract concluded with him/her; and
b) processing is automatized.

17.7.2. Among the data processing that are the subject of this information, the data processing presented in the following chapters meet the above conditions, so the right to data portability can be exercised with regard to them:

a) completed on the basis of consent:
3. Technical data processing related to ensuring the operation of information technology services based on consent;
4. Processing related to receiving and answering messages;
5. Processing related to sending newsletters;
6. Data management related to making direct sales through sending SMS and MMS messages;
7. Processing related to registration;

b) completed with the legal basis for the performance of the contract concluded with the User:
8. Data processing related to Users' contracting.

17.7.3. Practising the right to portability of data, User has the right – if it is technically practicable – to ask Controllers to forward information between each other directly.

17.8. Right to objection

17.8.1. User may object to the processing of his/her personal data based on legitimate interest at any time for reasons related to his/her own situation.

17.8.2. In such cases, Controller can handle personal information any longer only if Controller proves that there are obligatory rightful reasons for processing, having priority over User's interests, rights and freedoms, or reasons that are related to proposal, enforcement or defence of legal demands.

17.8.3. Among the data processing that are the subject of this information, the User can exercise his right to protest with respect to the data processing presented in the following chapters on data processing carried out with the legal basis of legitimate interest:
3. Technical data processing related to ensuring the operation of information technology services based on legitimate interest;
9. Data processing related to ordering on behalf of an organization in the case of a natural person acting on behalf of an organization;
14. Data transmission in connection with online payment).

18. Fulfilling of User's requests

18.1. Controller offers notification and taking actions for free, as described in Point 16. If User's request is obviously unfounded, or – especially for its repeated nature – exaggerated, Controller
a) might charge a reasonable price, or
b) might deny taking actions based on request,

considering data requested, or administrative costs of measures to be taken to fulfil request.

18.2. Controller informs User without any unreasonable delay, but maximum one month after receiving the request about actions that has been taken, including issuing copies of data. If necessary, considering the complexity of request and numbers of requests this deadline can be made longer with additional two months. Controller informs User about elongation of deadline together with indicating reasons of delay within one month after receiving the request. If concerned User sends their request electronically, Controller provides information electronically, except when concerned User asks for it in a different way.

18.3. If Controller does not take any steps as reaction to User's request, without delay but within maximum of one month after receiving the request, Controller informs User about reasons why there have been no actions taken, and about the possibility of filing a

complaint at Authority mentioned in Point 18 and can have the right to legal remedy described there as well.

18.4. User can hand in their request to Controller in any way that identifies them. Identifying Users who hand in a request is necessary because Controller can deal with only those requests that are entitled. If Controller has justified doubts about the identity of natural person handing in a request it can ask for other pieces of information to assure the identity of concerned User.

18.5. User can send their requests to Controller to the address **36 Küküllő Street, Helvécia 6034 Hungary (Magyarország, 6034 Helvécia, Küküllő u. 36.)** or to the e-mail address **info@totallsport.com** Controller considers requests sent in e-mail genuine only if it was sent from an e-mail address registered at Controller's database. However, using another e-mail address does not mean in observance of such requests. Time of receiving e-mails is the first day after the e-mail was sent.

19. Prosecution of rights

Concerned parties may practice their prosecution of rights based on Civil Code Act V of 2013 (Polgári Törvénykönyvről szóló 2013. évi V. törvény) and GDPR at a courthouse, and can turn to the National Authority for Data Protection and Freedom of Information:

Nemzeti Adatvédelmi és Információszabadság Hatóság
(National Authority for Data Protection and Freedom of Information)

Address: 9-11. Falk Miksa Street, Budapest 1055 Hungary (Magyarország, 1055 Budapest, Falk Miksa utca 9-11.)
Postal address: P.O. Box 9 Budapest 1363 Hungary (Magyarország 1363 Budapest, Pf. 9.)
Telephone: +36 1 391 1400
Fax: +36 1 391 1410
E-mail: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu/

In case choosing a process involving a courthouse, the lawsuit – based on concerned User's choice – can be initiated at the courthouse in concerned person's residence or place of stay, as courthouses are competent in confiscation of such a lawsuit.

Download/print the document: HERE

2024.10.01.

Goal Hungary Kft.