PRIVACY POLICY

SMARTPORT web application

1. Purpose of the Privacy Policy

The goal of our Privacy Policy is to provide all necessary information about processing your personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and assist the Data subjects in exercising their rights under Section 4.

The legal basis of our duty to communicate information is Article 12 of Regulation 2016/679 of the European Parliament and Council (hereinafter referred to as: GDPR) and the relevant Hungarian data protection regulations.

In the Privacy Policy, we may define you as "data subject", or "contact person of our business partners" in the following.

You may find further definitions concerning your personal data within the Appendix of the current Privacy Policy.

2. Data controller

Name	SCI-HÁLÓZAT TÁVKÖZLÉSI és HÁLÓZATINTEGRÁCIÓS Zrt.
Registry number	01 10 043883 (Hungarian Company registry)
Registered seat	1142 Budapest, Erzsébet királyné útja 125.
E-mail	info@scinetwork.hu
Telephone number	+36 1 467 7030
Representative of the data controller	István Lovas, CEO

hereinafter referred to as data controller.

3. Data processing concerning contacting and communication

It is possible to connect us through our availabilities located on the website. Also, by communicating with our business partners, we process the personal data of their contact person. The details of these processing are described hereunder.

3.1. Processed personal data and purpose of processing

SmartPort is a uniquely developed, innovative web application whose main purpose is the quick and easy control of individual ports, the planning of tasks around ports and ships, and the organization of shipmaster training. SmartPort is based on web technologies, so it can be accessed from anywhere in the world, even with a mobile phone. To do this, the web application uses Node.js with JavaScript and the MongoDB open source NoSQL database.

With the help of SmartPort, port operators can easily and transparently manage sailing clubs online, and the user side, ship owners or charterers can manage their shipping-related matters on a single interface.

SmartPort processes personal data within the framework of various modules as follows:

Port operation module

Categories of data	Rental/tenant data related to the processing of berth data. Data of the owner(s) related to the processing of the data of ships. Display map/port diagram: recording, replacing, removing the position of ships. Management of human resources, persons and users: personal data (depending on the role).
The purpose of the data processing	Operation of SmartPort, which is a uniquely developed, innovative web application, the main purpose of which is the quick and easy control of individual ports, the planning of tasks around ports and ships, and the organization of shipmaster training.
The legal basis for data processing	In relation to the processing of the data of berths and ships, with regard to the processing of the data of owners/tenants, Article 6 (1) point b of the GDPR, data processing is necessary for the fulfillment of a contract in which the data subject is one of the parties, or at the request of the data

	subject prior to the conclusion of the contract necessary to take the following steps. In the case of recording, replacing, and removing the position of ships, as well as the management of human resources, persons, and users, Article 6 (1) point f of the GDPR, data processing is necessary to enforce the legitimate interests of the data controller or a third party.
Data subjects include people under the age of 18 or with limited capacity	no
Special categories of personal information	no
Storage limitation	The Company processing personal data for the duration of the contract or legitimate interest.
Recipient	none
How does the organization get the data?	By the data subject or by using location-determining devices
Who is entitled to access the data within the organization?	CEO and office managers

Charter operation module:

Categories of data	Recording leases: assigning a tenant to a lease
The purpose of the data processing	Operation of SmartPort, which is a uniquely developed, innovative web application, the main purpose of which is the quick and easy control of individual ports, the planning of tasks around ports and ships, and the organization of shipmaster training.
The legal basis for data processing	With regard to the processing of tenants' data, Article 6 (1) point b of the GDPR, data management is necessary for the performance of a contract in which the data subject is one of the parties, or it is necessary to take steps at the request of the data subject prior to the conclusion of the contract.

Data subjects include people under the age of 18 or with limited capacity	no
Special categories of personal information	no
Storage limitation	The Company processing personal data for the duration of the contract.
Recipient	none
How does the organization get the data?	By the data subject.
Who is entitled to access the data within the organization?	CEO and office managers

Education module

Categories of data	Processing of course, exam, and other event data: instructor, ship, student data. Management of instructors (human resources): schedule based on calendar. Student data processing: application management (group, additional training), education-related documents, education history management.
The purpose of the data processing	Operation of SmartPort, which is a uniquely developed, innovative web application, the main purpose of which is the quick and easy control of individual ports, the planning of tasks around ports and ships, and the organization of shipmaster training.
The legal basis for data processing	With regard to student data, Article 6 (1) point a) of the GDPR is the consent of the data subject. In the case of the processing of instructor's data, Article 6 (1) point f) of the GDPR, data processing is necessary to enforce the legitimate interests of the data controller or a third party.
Data subjects include people under the age of 18 or with limited capacity	Yes
Special categories of personal information	Yes

Storage limitation	The Company processes personal data for as long as the consent of the data subject or legitimate interest exists.
Recipient	none
How does the organization get the data?	By the data subject.
Who is entitled to access the data within the organization?	CEO and office managers

3. Processors

We do not use additional data processors for data processing.

Our companies do not transfer your personal data above to any third country or international organization.

Automated decision making and profiling: none of this happens during data processing.

4. What are your rights?

5.1. Right to access

You have the right to obtain confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the information featured in point 3.

You have the right to access to the following information concerning the processing of your personal data:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from us rectification or erasure of personal data or restriction of processing of personal data concerning you or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- the existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

5.2. Right to rectification

You have the right to obtain from us without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

5.3. Right to erasure

You have the right to obtain from us the erasure of personal data concerning you without undue delay and we shall have the obligation to erase personal data without undue delay if it is

mandatory according to Article 17 of GDPR. The erasure of your personal data is obligatory for us in the following instances:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- you withdraw consent on which the processing is based, and where there is no other legal ground for the processing;
- you object to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

5.4. Right to be forgotten

If we made the personal data public and are obliged to erase your personal data, we inform controllers which are processing the personal data that you have requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

We do not make your personal data public.

5.5. Right to restriction of processing

You have the right to obtain from us restriction of processing if is obligatory according to Article 18 of GDPR. Such instances are the following:

- the accuracy of the personal data is contested by you, for a period enabling us to verify the accuracy of the personal data;
- the processing is unlawful and you oppose the erasure of the personal data and requests the restriction of their use instead;
- we no longer need the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defense of legal claims;

If you obtain restriction of processing in accordance with the above, we inform you before the restriction of processing is lifted.

5.6. Right to data portability

You have the right to receive the personal data concerning you, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from us if is possible according to Article 20 of GDPR. Where technically feasible, you have the right to have the personal data transmitted directly from us to another controller.

5.7. Right to object

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on point (f) of Article 6(1) of GDPR (see: point 3.2. of the current policy). In such case, we no longer process the personal data unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

5.8. Right to lodge complaint

You have the right to appeal to the Hungarian courts and to make a complaint to the

Hungarian Supervisory Authority (https://naih.hu/)

Post address: 1363 Budapest, Pf.: 9.

Address: 1055 Falk Miksa utca 9-11.

Phone: +36 (1) 391-1400

E-mail: ugyfelszolgalat@naih.hu

6. Measures and notification

6.1. Informing Data subjects

We communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 of GDPR to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. We also inform you about those recipients on the request of yours.

6.2. Mode and deadline of notification

We provide information on action taken on a request under Articles 15 to 22 of GDPR to you without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We inform you of any such extension within one month of receipt of the request, together with the reasons for the delay. Where you make the request by electronic form means, we provided the information by electronic means where possible, unless you request it otherwise.

If we do not take action on your request, we inform you without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (see point 4.7.).

6.3. Monitoring

If we have reasonable doubts concerning the identity of the natural person making the request, we may request the provision of additional information necessary to confirm the identity of the data subject.

6.4. Costs of measures and notifications

We provide you information and take the necessary measures free of charge.

If your requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested or we refuse to act on your request.

7. Cookies

7.1. Cookies in general

A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

Cookies can be used by web servers to identify and track users as they navigate different pages on a website and identify users returning to a website.

7.2. Our cookies

We use Google Analytics to analyse the use of our website.

Our analytics service provider generates statistical and other information about website use by means of cookies.

The information generated relating to our website is used to create reports about the use of our website.

Our analytics service provider's privacy policy is available at: https://unas.hu/adatkezelesi-tajekoztato

7.3. Blocking cookies

Most browsers allow you to refuse to accept cookies; for example:

- in Internet Explorer (version 11) you can block cookies using the cookie handling override settings available by clicking "Tools", "Internet Options", "Privacy" and then "Advanced";
- in Firefox (version 39) you can block all cookies by clicking "Tools", "Options", "Privacy", selecting "Use custom settings for history" from the drop-down menu, and unticking "Accept cookies from sites"; and

- in Chrome (version 44), you can block all cookies by accessing the "Customise and control" menu, and clicking "Settings", "Show advanced settings" and "Content settings", and then selecting "Block sites from setting any data" under the "Cookies" heading.

Blocking all cookies will have a negative impact upon the usability of many websites.

If you block cookies, you will not be able to use all the features on our website.

7.4. Deleting cookies

You can delete cookies already stored on your computer; for example:

(a) in Internet Explorer (version 11), you must manually delete cookie files (you can find instructions for doing so at http://windows.microsoft.com/en-gb/internet-explorer/delete-manage-cookies#ie=ie-11);

(b) in Firefox (version 39), you can delete cookies by clicking "Tools", "Options" and "Privacy", then selecting "Use custom settings for history" from the drop-down menu, clicking "Show Cookies", and then clicking "Remove All Cookies"; and

(c) in Chrome (version 44), you can delete all cookies by accessing the "Customise and control" menu, and clicking "Settings", "Show advanced settings" and "Clear browsing data", and then selecting "Cookies and other site and plug-in data" before clicking "Clear browsing data".

Deleting cookies will have a negative impact on the usability of many websites.

8. Data security

We secure your personal information from unauthorized access, use or disclosure. We secure the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information (such as connection data) is transmitted to other Web sites, it is protected through the use of encryption, such as the Secure Socket Layer (SSL) or HTTPS protocol.

Our employees and the employees of the data processors have the right to get acquainted with the personal data of the User, to the extent necessary, for the performance of the tasks which belong to their job. We make all technical and organizational measures that guarantee the security of the data.

8.1. Organizational measures

We provide access to our IT systems with personalized rights. The "necessary and sufficient rights" principle applies to the allocation of accesses, consequently all employees may use our IT systems and services only to the extent necessary for the performance of their duties, with the appropriate rights and for the required time. Access to IT systems and services can only be granted to a person who is not restricted for security or other reasons (e.g. conflicts of interest) and who has the professional, business and information security knowledge required to use it securely.

We and the data processors undertake strict confidentiality rules in a written statement, and we are obliged to act in accordance with these confidentiality rules during the course of our activities.

8.2. Technical measures

The data is stored, with the exception of the data stored by our data processors, on our own devices, in a data center. The IT devices which store data are located in an isolated, separate closed server room, protected by a multi-stage access control system subject to authorization control.

We protect our internal network with multi-level firewall protection. In all cases, a hardware firewall (border protection device) is located at the entry points of the applied public networks. The data is stored redundantly, that is, in several places, so it is protected from destruction, loss, damage, or illegal destruction due to the failure of the IT device.

Our internal networks are protected from external attacks with a multi-level, active protection against complex malicious code (e.g. virus protection). The external access to the IT systems and databases is operated by us via an encrypted data connection (VPN).

We do steps to ensure that the IT tools and software continuously comply with the generally accepted technological solutions in the market.

We develop systems, during our development, in which logging can be used to control and monitor the operations performed, and to detect incidents, such as unauthorized access.

Our server is protected and closed, located on the dedicated servers of the hosting provider.

9. Other provisions

9.1. Processing for different purpose

If we intend to further process the personal data for a purpose other than that for which the personal data were collected, we provide the you prior to that further processing with information on that other purpose and with any relevant further information.

9.2. Data protection

We secure your personal information from unauthorized access, use or disclosure. We secure the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information (such as connection data) is transmitted to other Web sites, it is protected through the use of encryption.

9.3. Record of processing

To comply with section 30 of GDPR, we maintain a record of processing activities under our responsibility.

9.4. Data breaches

Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. In case of data breach, we act according to section 33 and 34 of GDPR.

9.5. Changes to our Privacy Policy

We will occasionally update this Privacy Policy to reflect feedback. We encourage you to periodically review this Policy to be informed of how we are protecting your information.

Date: 17.October, 2022.

István Lovas CEO

Data Controller

10. Appendix - Definitions

- 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

- 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

- 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

- 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

- 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

- group of undertakings' means a controlling undertaking and its controlled undertakings;

- 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

- 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

- 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;