DATA MANAGEMENT AND PRIVACY POLICY

[based on GDPR]

Organization Name: Lake Spirit Kft.
Registered Office: 1141 Budapest, Paskál utca 36/a
Tax Number: 28742137-2-42
Email: info@lakespirit.hu
Central Phone Number: +36 30 154 5644
Website: https://www.lakespirit.hu/

This policy is reviewed and maintained annually based on legislative changes.

Effective Date: September 1, 2023
Applicable Until: September 1, 2030

Table of Contents

Interpretative Provisions

Data Processor	A natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the Data Controller.
Data Processing	Any operation or set of operations performed on personal data or data sets, whether automated or not, 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.
Data Controller	The Company, as well as any natural or legal person, public authority, agency, or any other body that, alone or jointly with others, determines the purposes and means of processing personal data. Where the purposes and means of data processing are determined by Union or Member State law, the Data Controller or the specific criteria for its designation may be provided by Union or Member State law.
Data Protection Incident	A security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, transmitted, stored, or otherwise processed personal data.
Biometric Data	Any personal data resulting from specific technical processing related to the physical, physiological, or behavioral characteristics of a natural person that allows or confirms the unique identification of that natural person, such as facial images or fingerprint data.
Recipient	A natural or legal person, public authority, agency, or another body to which personal data is disclosed, whether or not it is a third party. However, public authorities that may access personal data in accordance with Union or Member State law within the framework of a specific investigation are not considered recipients; the processing of such data by those public authorities must comply with applicable data protection regulations in line with the purposes of data processing.
Health Data	Personal data related to the physical or mental health of a natural person, including data about healthcare services provided to the person that reveal information about their health status.
Data Subject	The natural person whose personal data is being processed.
Data Subject's Consent	The freely given, specific, informed, and unambiguous indication of the data subject's will by which they, through a statement or a clear affirmative action, signify agreement to the processing of their personal data.
EU Member State	The member states of the European Union, including Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

Supervisory Authority	An independent public authority established by an EU member state in accordance with Article 51 of the GDPR.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation).
Genetic Data	Any personal data relating to the inherited or acquired genetic characteristics of a natural person that provide unique information about that person's physiology or health and that result primarily from the analysis of a biological sample taken from the individual.
Third Party	A natural or legal person, public authority, agency, or any other entity that is not the data subject, controller, processor, or a person authorized to process personal data under the direct authority of the controller or processor.
Special Data	Personal data that belong to special categories of personal data.
International Organization	An entity subject to international public law, its subordinate bodies, or any other organization established or based on an agreement between two or more countries.
Profiling	Any form of automated processing of personal data used to evaluate certain personal characteristics related to a natural person, particularly those concerning work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
Personal Data	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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Special Categories of Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic and biometric data processed for the purpose of uniquely identifying a natural person, health data, and data concerning a natural person's sex life or sexual orientation.
Company	Lake Spirit Kft., as the data controller.

1. Purpose of the Policy

The purpose of this Data Management Policy is to introduce and consistently apply measures that ensure the accurate and secure processing of personal data of Employees (hereinafter: Data Subjects) in compliance with applicable EU and national data protection regulations. This policy ensures a uniform approach to data processing at the level of Lake Spirit Kft (hereinafter: the Company).

Additionally, the Data Management Policy provides concise, transparent, and easily accessible information for Data Subjects regarding access to their personal data processed by the Company. It also establishes regulations and provides information on the Company's measures to ensure the rights of Data Subjects.

.

2. Scope of the Policy

Personal Scope

This policy applies to the Company and all natural persons whose personal data are subject to the Company's data processing activities. The data processing activities outlined in this policy pertain to personal data of natural persons only. The policy does not cover data processing related to legal entities or businesses established as legal entities, including data such as the name, form, and contact details of a legal entity. Legal entities include associations, business companies, cooperatives, unions, and foundations.

Temporal Scope

This policy remains in effect from the date of its establishment until further notice or until it is revoked.

3. Data Processing Principles

Before initiating any personal data processing, it must always be carefully assessed whether such processing is genuinely necessary. Personal data may only be processed if it is unequivocally justified that the intended purpose cannot be achieved by other means.

The Company is obligated to handle personal data lawfully, fairly, and transparently. No individual shall face any disadvantage due to initiating proceedings, seeking legal remedies, or submitting a report to the Company or any authority specified in this Policy. Likewise, no adverse consequences shall result from refusing or withdrawing consent in cases where data processing is based on consent.

The collection of personal data must always serve a specific, clear, and lawful purpose. The Company must prevent or, if necessary, discontinue any data processing that is inconsistent with the stated purpose. The Company is only

authorized to process personal data to the extent necessary and must delete any personal data once the purpose of processing ceases to exist or when the legal basis for processing is no longer valid.

3.1 The Company is obligated to implement control mechanisms that ensure, both preemptively and retrospectively, that:

3.2 Personal data comply with the purposes of data processing at the time of collection and throughout the entire processing period.

3.3 The extent of data processing is limited to what is necessary, both in terms of the scope of data and the duration of processing.

3.4 The personal data managed by the Company must be accurate and up to date. The Company is required to take all reasonable measures to ensure the accuracy of personal data, including:

3.5 The immediate deletion of unnecessary or outdated personal data.

3.6 The correction or deletion of inaccurate personal data.

3.7 Personal data must be stored in a form that allows identification of Data Subjects only for the time necessary to achieve the purposes of processing.

3.8 Data processing must be carried out in a manner that ensures the adequate security of personal data through appropriate technical and organizational measures, protecting against unauthorized or unlawful processing, accidental loss, destruction, or damage.

3.9 2. Lawfulness of Data Processing

3.10 A correct determination of the legal basis for data processing and compliance with the conditions associated with the chosen legal basis are prerequisites for lawful data processing. The requirement of lawfulness, in a narrow sense, presupposes the existence of an appropriate legal basis. In a broader sense, it means that personal data processing can only take place in accordance with the laws applicable to the given legal basis.

3.11 Based on its activities, the Company may choose from the following key legal bases for processing the personal data of Data Subjects, depending on the nature and circumstances of data processing. The legal bases mentioned in the first subsection apply to all personal data, except for special categories of personal data, while the second subsection contains specific provisions regarding the legal bases applicable to special categories of personal data.

3.12 2.1 Personal Data (excluding special categories of data)

3.13 The Company may process the personal data of the Data Subject—excluding special categories of data—on the following legal bases:

3.14 Consent: The Company may process personal data based on consent if the voluntariness of consent can be proven. If the Company processes the personal data of a child under the age of 16 in connection with information society services offered directly to them, such processing is generally lawful only if and to the extent that parental consent or authorization is given. The Data Subject provides consent voluntarily and has the right to withdraw it at any time. Withdrawal does not affect the lawfulness of processing carried out prior to the withdrawal.

3.15 Performance of a contract or steps prior to entering a contract: This legal basis applies when data processing is necessary for the performance of a contract (e.g., a service agreement, employment contract, or study agreement) in which the Data Subject is a party, or when processing is necessary for taking steps at the Data Subject's request before entering into a contract.

3.16 Compliance with a legal obligation: Data processing required by EU or national law.

3.17 Legitimate interest: This includes data processing necessary to protect the legitimate interests of the Company or a third party. The Company or the third party's legitimate interest is recorded in the relevant data processing notice.

3.18 Other legal bases: Data processing may also be based on the Data Subject's or another natural person's vital interests, public interest, or the exercise of official authority vested in the Company.

3.19 If the Company collects data directly from the Data Subject and the Data Subject does not provide the data required for processing under the above legal bases, the possible consequences may include the refusal or impossibility of preparing or performing a contract (e.g., failure to establish an employment relationship). If the Data Subject provides only partial data, the Company must assess whether the lack of full data prevents the conclusion or continuation of the contract. In the case of contract-based data processing, the Company may only apply the legal consequences of impossibility if it can prove that the contract cannot be performed without the provided data.

1.21 Special Categories of Data

Due to the fundamental rights and freedoms of natural persons, special categories of data are inherently sensitive and pose risks, requiring distinguished protection.

The Company may process the Data Subject's special categories of data—including, primarily, health-related data—based on the following purposes and legal grounds:

a) GDPR Article 9(2)(a): The Data Subject may provide consent for the processing of their personal data, provided that the voluntary nature of the consent can be proven (a sample of this is included in Annex 1). The Data Subject provides consent on a voluntary basis and has the right to withdraw it at any time. The withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

b) GDPR Article 9(2)(b): If authorized by Union or Member State law, or a collective agreement under Member State law, the Company may process personal data to fulfil its obligations and exercise specific rights arising from legal regulations related to employment, social security, and social protection.

c) GDPR Article 9(2)(f): This legal basis applies if the processing of special categories of data is necessary for the establishment, exercise, or defence of legal claims.

2. The Company's Obligation to Provide Information and Its Measures

The Company is required to provide certain information to the Data Subject in a concise, transparent, easily accessible, clear, and comprehensible form and to inform the Data Subject of their rights. Furthermore, upon request and in compliance with specific procedural rules, the Company may take measures accordingly.

2.1 Privacy Policy

Depending on whether the personal data is collected from the Data Subject, the Company must provide the Data Subject with certain information regarding data processing. The general and specific rules of this privacy policy are summarized in the following subsections.

2.1.1 General Rules

Under its obligation to provide information, the Company must inform the Data Subject of the following:

a) The identity and contact details of the Company and, if applicable, its representative.
b) The purpose and legal basis of the intended data processing.
c) In cases where processing is based on GDPR Article 6(1)(f), the legitimate interests of the Company or a third party.
d) If applicable, the recipients or categories of recipients of the personal data.
e) If applicable, the fact that the Company intends to transfer personal data to a third country or an international organization, along with the existence or absence of an adequacy decision by the European Commission, or in the case of transfers under GDPR Articles 46, 47, or 49(1)(2), the appropriate safeguards and means of obtaining a copy of them or where they are available.
f) The duration of personal data storage or, if not possible, the criteria for determining this duration.
g) The Data Subject's right to request access to, rectification, erasure, or restriction of the processing of personal data, as well as the right to object to such

processing and the right to data portability.
h) If processing is based on GDPR Article 6(1)(a) or Article 9(2)(a), the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
i) The right to lodge a complaint with a supervisory authority.
j) The fact of automated decision-making, including profiling as mentioned in GDPR Article 22(1) and (4), as well as, in such cases, meaningful information about the logic involved and the potential significance and consequences of such processing for the Data Subject.

2.1.2 Information to Be Provided When Data Is Collected from the Data Subject

If the Company collects personal data directly from the Data Subject, in addition to the above, it must inform them whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for entering into a contract, whether the Data Subject is obliged to provide the personal data, and the possible consequences of failing to do so.
This information must be provided at the time of data collection. However, if the Data Subject already has the above information, it is not necessary to provide it again.

2.1.3 Information to Be Provided When Data Is Not Collected from the Data Subject

If the Company collects personal data from a source other than the Data Subject, in addition to the above, it must inform them about the categories of personal data and the source of the personal data, including whether the data originates from publicly accessible sources.

The Company must provide this information:
a) Within a reasonable period after obtaining the personal data, but no later than one month.
b) If the personal data is used to contact the Data Subject, at the latest upon first contact.
c) If the personal data is expected to be disclosed to another recipient, at the latest when the personal data is first disclosed.

The Company is not required to provide this information if:
a) The Data Subject already has the information.
b) Providing the information proves impossible or would require disproportionate effort, particularly in cases where processing is carried out for purposes of public interest archiving, scientific or historical research, or statistical purposes, under GDPR Article 89(1), and if providing the information would likely make achieving these purposes impossible or seriously impair them. In such cases, the Company must take appropriate measures, including making the information publicly available, to protect the rights, freedoms, and legitimate interests of the Data Subject.
c) The acquisition or disclosure of the data is expressly required by Union or Member State law applicable to the Company, which provides for appropriate measures to protect the Data Subject's legitimate interests.
d) The personal data must remain confidential due to an obligation of professional secrecy prescribed by Union or Member State law, including a statutory duty of confidentiality.

2.2 Persons Authorized to Access the Data

Personal data may be accessed by the Company's employees who have access rights related to the relevant data processing purpose, as well as individuals or organizations performing data processing activities on behalf of the Company under service agreements, to the extent necessary for their activities.
The list of data processors is included in Annex 3 of the regulations.

2.3 Data Subject Rights

The Data Subject may request access to, rectification, erasure, or restriction of the processing of their personal data from the Company, and may object to the processing of such personal data. The Data Subject also has the right to data portability, legal remedies, and the right to make decisions regarding automated decision-making, including profiling.
The Company must provide information on certain Data Subject rights as part of the privacy policy mentioned in Section 5.1.

2.3.1 Right to Rectification

The Data Subject has the right to request the controller to rectify inaccurate personal data concerning them without undue delay. Considering the purposes of processing, the Data Subject has the right to request the completion of incomplete personal data, including by means of a supplementary statement.

2.3.2 Right to Erasure (“Right to Be Forgotten”)

(1) The Data Subject has the right to request the controller to erase personal data concerning them without undue delay, and the controller is obliged to erase personal data without undue delay if one of the following grounds applies:

- The personal data is no longer necessary for the purposes for which it was collected or otherwise processed.
- The Data Subject withdraws their consent under GDPR Article 6(1)(a) or Article 9(2)(a), and there is no other legal basis for processing.

The data subject objects to data processing pursuant to Article 21(1) of the Regulation (right to object) and there is no overriding legitimate reason for processing, or the data subject objects to data processing pursuant to Article 21(2) of the Regulation (objection to personal data processing for direct marketing purposes);
The personal data has been processed unlawfully;
The personal data must be deleted to comply with a legal obligation under Union or Member State law applicable to the data controller;
The personal data was collected in relation to the offering of information society services referred to in Article 8(1).

(2) If the data controller has made the personal data public and is obliged to delete it upon the data subject's request, the data controller shall take reasonable steps—taking into account available technology and implementation costs—including technical measures to inform other data controllers processing the data that the data subject has requested the deletion of any links to, copies, or replications of that personal data.

(3) Paragraphs (1) and (2) do not apply if the processing is necessary:

- For exercising the right to freedom of expression and information;
- For compliance with a legal obligation that requires processing under Union or Member State law, or for performing a task carried out in the public interest or in the exercise of official authority vested in the controller;
- For reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (i), and Article 9(3);
- For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1), where the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the processing objectives;
- For the establishment, exercise, or defence of legal claims.

1.20.1 Right to Restriction of Processing

(1) The data subject has the right to obtain from the controller a restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject, in which case the restriction applies for the period necessary for the controller to verify the accuracy of the personal data;

- The processing is unlawful, and the data subject opposes the deletion of the data and requests instead the restriction of its use;

- The controller no longer needs the personal data for processing purposes, but the data subject requires it for the establishment, exercise, or defence of legal claims;

- The data subject has objected to processing under Article 21(1); in this case, the restriction applies until it is determined whether the controller's legitimate grounds override those of the data subject.

(2) If processing is restricted under paragraph (1), such personal data shall, except for storage, only be processed with the data subject's consent, for the establishment, exercise, or defence of legal claims, for the protection of another natural or legal person's rights, or for important public interests of the Union or a Member State.

(3) The controller shall inform the data subject who requested restriction before lifting such restriction.

1.20.2 Obligation to Notify Rectification, Deletion, or Restriction of Processing

(1) The controller shall communicate any rectification, deletion, or restriction of processing to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.

(2) The controller shall inform the data subject about those recipients upon request.

1.20.3 Right to Data Portability

(1) The data subject has the right to receive personal data concerning them, which they have provided to a controller, in a structured, commonly used, and machine-readable format, and has the right to transmit that data to another controller without hindrance from the controller to whom the personal data was provided, if:

- The processing is based on consent under Article 6(1)(a) or Article 9(2)(a) (explicit consent for special categories of data), or on a contract under Article 6(1)(b); and

- The processing is carried out by automated means.

(2) When exercising the right to data portability, the data subject has the right to have personal data transmitted directly from one controller to another, where technically feasible.

(3) The exercise of this right shall not adversely affect the rights and freedoms of others.

1.20.4 Right to Object

(1) The data subject has the right to object, on grounds relating to their particular situation, at any time to the processing of personal data concerning them based on the necessity of processing for public interest tasks or for legitimate interests of the controller or third parties (Article 6(1)(e) or (f)), including profiling based on these provisions. In such cases, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds that override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defence of legal claims.

(2) If personal data is processed for direct marketing purposes, the data subject has the right to object at any time to such processing, including profiling related to direct marketing.

(3) If the data subject objects to processing for direct marketing purposes, their personal data shall no longer be processed for such purposes.

(4) The right mentioned in paragraphs (1) and (2) must be explicitly brought to the attention of the data subject no later than the first communication, and must be presented clearly and separately from other information.

(5) In the context of information society services and notwithstanding Directive 2002/58/EC, the data subject may exercise their right to object by automated means using technical specifications.

(6) Where personal data is processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject has the right to object to processing for reasons related to their situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

1.20.5 Right to Avoid Automated Decision-Making

(1) The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

(2) This right does not apply if the decision:

- Is necessary for entering into or performing a contract between the data subject and the controller;

- Is authorized by Union or Member State law applicable to the controller, which also lays down suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests; or

- Is based on the data subject's explicit consent.

(3) In the cases mentioned in paragraph (2)(a) and (c), the controller must implement appropriate measures to safeguard the data subject's rights, including at least the right to obtain human intervention, express their point of view, and contest the decision.

(4) Decisions must not be based on special categories of personal data under Article 9(1) unless Article 9(2)(a) or (g) applies and appropriate safeguards are in place.

1.20.6 Right to Lodge a Complaint and Seek Legal Remedies

Right to Lodge a Complaint

If the data subject believes that the processing of their personal data by the company violates applicable data protection regulations, especially GDPR, they have the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information (NAIH).

NAIH Contact Information:
Website: http://naih.hu/
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Mailing address: 1530 Budapest, P.O. Box 5
Phone: +36-1-391-1400
Fax: +36-1-391-1410
Email: ugyfelszolgalat@naih.hu

The data subject also has the right to lodge a complaint with another supervisory authority in the EU member state of their habitual residence, workplace, or the place of the alleged infringement.

Judicial review of the decision of the supervisory authority or other legal remedy

The Data Subject and the Company shall have the right to an effective judicial remedy against a legally binding decision of the supervisory authority concerning them, in particular against a decision of the supervisory authority to exercise its powers of investigation, correction and authorisation, or to consider complaints as unfounded or to reject them. However, the right to an effective judicial remedy shall not apply to legally binding decisions of the supervisory authorities.

Furthermore, the Data Subject shall have the right to an effective judicial remedy if the supervisory authority competent pursuant to Article 55 or 56 of the GDPR does

not deal with the complaint or does not inform the Data Subject within three months of the progress of the procedure or the outcome of the complaint submitted to it.

Proceedings against the supervisory authority shall be brought before the courts of the EU Member State in which the supervisory authority is established. Right to Seek Legal Remedies (Right to File a Lawsuit)

The Data Subject, regardless of their right to file a complaint, may bring a legal action if their rights under the GDPR have been violated in the course of processing their personal data.

A lawsuit against the Company, as a data controller with domestic operations, can be filed before a Hungarian court.

Under Section 22(1) of the current Infotv., the Data Subject may also initiate proceedings before the competent court based on their place of residence. Information about Hungarian courts is available at the following link: http://birosag.hu/torvenyszekek.

Since the Company does not qualify as a public authority exercising official powers of an EU Member State, the Data Subject may also file the lawsuit before the competent court in their habitual residence Member State if that residence is in another EU country.

1.21 Procedural Rules

The Company must comply with the obligations and measures set out in this document. In addition to the specific rules defined above, the Company shall act in accordance with the following provisions.

1.21.1 Processing of Requests

For the measures requested in relation to the specified data subject rights, the following procedural rules shall apply:

- The Data Subject may submit their request to the employee holding the Managing Director position.
- Requests must be submitted in writing, either via electronic mail or in paper form, and shall be assessed based on their content. If the request is submitted electronically, the response should also be provided electronically unless the Data Subject requests otherwise.
- The Data Subject must specify in their request which personal data the Company should take action on.
- The Company is obligated to process the written request within one (1) month from receipt. If necessary, considering the complexity of the request or the number of ongoing requests, the Company may extend the processing time by an additional two (2) months. The Data Subject must be

informed about the extension and the reasons for the delay within one (1) month of receiving the request.

- If the Data Subject's request is justified, the Company shall carry out the requested action within the procedural deadline and provide written confirmation of the execution to the Data Subject.
- If the Company does not take action on the Data Subject's request, it must inform the Data Subject without undue delay, but no later than one (1) month from receipt, explaining the reasons for not taking action and informing the Data Subject of their right to lodge a complaint with a supervisory authority and seek judicial remedies.

2. Restrictions

(1) Union or Member State law applicable to the controller or processor may, by legislative measures, restrict the scope of the rights and obligations set out in Articles 12–22 and Article 34, as well as the rights and obligations defined in Article 5, provided that the restriction respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to protect:

a. National security;
b. Defence;
c. Public security;
d. Prevention, investigation, detection, or prosecution of criminal offenses, including enforcement of criminal penalties, and protection against and prevention of threats to public security;
e. Other important public interests of the Union or a Member State, especially economic or financial interests, including monetary, budgetary, and taxation matters, public health, and social security;
f. Judicial independence and judicial proceedings;
g. Prevention, investigation, detection, and prosecution of ethical breaches in regulated professions;
h. Supervisory, inspection, or regulatory functions related to public authority tasks in the cases mentioned in points (a)–(e) and (g);
i. Protection of the rights and freedoms of the data subject or others;
j. Enforcement of civil law claims.

(2) The legislative measures mentioned in paragraph (1) shall include, where appropriate, detailed provisions at least on:

a. The purposes of processing or categories of processing;
b. The categories of personal data;
c. The scope of the imposed restrictions;
d. Safeguards to prevent misuse, unauthorized access, or unauthorized disclosure;
e. The identification of the controller or categories of controllers;
f. The storage period of the data and applicable safeguards, considering the nature, scope, and purposes of processing;
g. Risks to the rights and freedoms of the data subjects;

h. The right of data subjects to be informed about the restriction unless this would compromise its purpose.

3. Data Transfers

The Company may transfer personal data of Data Subjects for specific purposes, particularly:

- Fulfilling a contract with a third party;
- Complying with legal obligations;
- Fulfilling employer obligations arising from employment relationships.

Except in cases where data transfers are mandated by law, the Company shall transfer personal data only to recipients:

- Located within the European Union; or
- That provide adequate guarantees that their data processing complies with GDPR requirements.

If the Company transfers personal data to a third country (outside the EU) or an international organization, it must ensure that the recipient provides a level of protection equivalent to that ensured by the Company, in compliance with Chapter V of the GDPR.

If the data transfer occurs to a third country or international organization that does not provide an adequate level of data protection under Chapter V of the GDPR (e.g., some Asian or African countries), such a transfer may only take place without the Data Subject's consent if it meets the criteria set out in Article 49 of the GDPR. Otherwise, the explicit consent of the Data Subject is required for the transfer.

---

4. Data Breach Management

In the event of a data breach, the Company must comply with the following regulations and act according to the following rules.

4.1 Notification to the Supervisory Authority

If a data breach occurs involving the Company’s processed data, it must be reported to the supervisory authority without undue delay, and, if feasible, within 72 hours of becoming aware of the breach. The notification must include at least the following details:

a) Nature of the data breach, including:

- Categories and approximate number of affected data subjects;
- Categories and approximate number of affected data records.

b) Contact details of the responsible person who can provide further information.

c) Potential consequences of the data breach.

d) Measures taken or proposed by the controller to remedy the breach, including steps taken to mitigate potential negative effects.

If it is not possible to provide all the required information at once, it may be submitted in phases, without undue delay.

If the notification is not made within 72 hours, a justification for the delay must be provided.

1.21 Notification of Data Subject

If a data subject, especially an employee of the company, learns about a data protection incident, they must immediately notify the company's representative.

In all cases where the data protection incident is likely to result in high risk to the rights and freedoms of any data subject(s) and the company becomes aware of the incident, it is obligated to inform the data subject(s) without undue delay. The notification must clearly and understandably include: a) the nature of the data protection incident,
b) the name and contact details of the person providing further information,
c) the likely consequences of the data protection incident,
d) the measures the company has taken or plans to take to address the data protection incident, including any actions aimed at mitigating any adverse consequences resulting from the incident.

Notification to the data subject is not required if any of the following conditions are met: a) the company has implemented appropriate technical and organizational protective measures, and these measures were applied to the personal data affected by the data protection incident, particularly measures such as encryption that make the data unintelligible to unauthorized persons,
b) after the data protection incident, the company has taken additional measures that ensure the likely high risk to the data subject's rights and freedoms is no longer likely to occur,
c) notification would require disproportionate effort. In such cases, the data subjects should be informed publicly, through commonly used means of communication, or similar measures should be taken to ensure effective notification.

If the company has not notified the data subject about the data protection incident, the supervisory authority, after assessing whether the data protection incident is likely to result in high risk, may order the notification of the data subject or confirm that any of the above conditions are met, and thus, notification to the data subject is not necessary.

2. Data Processing Records

9.1 Record of Data Processing Activities

The company and its representative are required to keep a written record of data processing activities under their responsibility, including electronic documents, in accordance with Article 30 of the GDPR. This record must contain the following information: a) the name and contact details of the company,
b) the purposes of the data processing,
c) a description of the categories of data subjects and personal data,
d) the categories of recipients with whom personal data is or will be shared,

including third-country recipients or international organizations,
e) if applicable, information about the transfer of personal data to third countries or international organizations, including the identification of the third country or international organization and, in the case of transfers under the second subparagraph of Article 49(1), a description of the appropriate safeguards,
f) where possible, the time limits set for the erasure of various categories of data,
g) where possible, a general description of the technical and organizational measures referred to in Article 32(1).

The company and its representative must make the record available to the supervisory authority upon request.

9.2 Record of Data Protection Incidents

The company records data protection incidents with the following information: a) the facts relating to the data protection incident,
b) the impact of the incident,
c) the measures taken to remedy it.

The supervisory authority may inspect this record to verify compliance with the provisions of Article 33 of the GDPR.

3. Data Protection Impact Assessment

During the data protection impact assessment, the company must conduct an impact assessment for data processing activities that are likely to result in high risk to the rights and freedoms of data subjects. The impact assessment must include at least the following information: a) a systematic description of the planned data processing operations and the purposes of the processing, including any legitimate interests pursued by the controller,
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes,
c) an assessment of the risks to the rights and freedoms of data subjects,
d) the measures taken to address the risks, including safeguards, security measures, and mechanisms to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons.

4. Data Processing Activities in Connection with Employment

4.1 Data Processing Before the Establishment of Employment

Data processing before the establishment of employment occurs in connection with the recruitment procedure and the assessment of fitness for the job.

For further details regarding data processing before the establishment of employment, please refer to section 8.1 and 8.2 of this policy.

4.1.1 Data Processing During Fitness Assessment

According to Section 10(1) of the Labor Code, two types of fitness assessments may be applied to employees: assessments required by employment regulations and those not required by employment regulations but necessary for the exercise of a right or the fulfillment of an obligation specified by employment regulations.

In both cases, employees must be informed about the purpose of the fitness assessment, the tools and methods used for the assessment, and, if applicable, the legal basis for the assessment. The employer may only receive information about whether the employee is fit for the job, and if so, what conditions need to

be met. However, the employer is not allowed to access the full details or documentation of the assessment.

The legal basis for data processing is the employer's legitimate interest. The purpose of data processing is to determine suitability for the job and to establish an employment relationship.

The duration of data processing is three years after the termination of employment.

4.2 Data Processing During Employment

The company processes employee personal data based on the employer's legitimate interest, the fulfillment of legal obligations, and the performance of the contract. Before starting data processing, the company must inform the employee about the legal basis and purpose of the processing.

The categories of personal data processed by the company include: a) name,
b) address, temporary address, postal address,
c) contact details, phone number, email address,
d) social security number, tax ID number, personal ID number,
e) salary amount,
f) bank account number,
g) deductions, withholdings, and their bank account numbers,
h) children, dependents, and their social security numbers.

The data subjects are the employees of the company.

3.20.1 The recipients of the personal data recorded above are: the person exercising the employer's authority, the Enterprise's employees performing personnel activities, accounting, payroll tasks, and data processors.

3.20.2 Purpose of data management: fulfilment of obligations arising from employment, (payment of wages), exercise of rights arising from employment. Establishment, termination of employment.

3.20.3 Duration of data management: 3 years after the termination of employment.

3.20.4

3.20.5 2. Other activities and data areas affected by data management

3.20.6 2.1 Data management based on legal obligation

3.20.7 2.1.1 Data management related to the fulfilment of anti-money laundering obligations

3.20.8 The Enterprise complies with Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing. Pursuant to Section 6 (1) of the Act on the Identification of a Natural Person Acting on Behalf of or on Behalf of a Customer, the Company is obliged to identify and verify the identity of a natural person acting on behalf of or on behalf of a customer when establishing a business relationship, in the event of data, facts or circumstances indicating money laundering or terrorist financing, if customer due diligence has not yet been carried out; and if there is any doubt about the authenticity or adequacy of previously recorded customer identification data.

3.20.9 The Company is obliged to record the following data during identification: the natural person acting on behalf of or on behalf of a customer

3.20.10 a) family name and first name;

3.20.11 b) family name and first name at birth;

3.20.12 c) nationality;

3.20.13 d) place and date of birth;

3.20.14 e) mother’s birth name;

3.20.15 f) address, or in the absence thereof, place of residence;

3.20.16 g) type and number of the identification document.

3.20.17 The scope of data processing: natural persons acting on behalf of or on behalf of a customer.

3.20.18 The Company’s manager or employee designated for customer due diligence is entitled to access personal data. The Company is entitled to process personal data recorded during customer due diligence for 8 years from the termination of the contract (business relationship).

3.20.19 2.1.2 Data processing necessary for the fulfilment of accounting obligations

3.20.20 The legal basis for the processing of the data of the Company’s natural person customers, customers, and suppliers is the fulfilment of a legal obligation, (Act CXXVII of 2007, Section 159 (1)) the purpose of using the data is to determine the mandatory data content of the invoice, issue an invoice, and perform related accounting tasks.

3.20.21 The scope of data processing: the Company’s natural person customers, customers, and suppliers.

3.20.22 The scope of the processed data: the name, address, tax number of the Company's natural person clients, buyers, suppliers

3.20.23 The manager and employees performing invoice issuance as a job task, the manager and employee performing accounting activities are entitled to access the personal data. The Company is entitled to process the personal data recorded in the course of fulfilling the legal obligation indicated above for 8 years from the termination of the contract (business relationship).

3.20.24 Data processing related to the fulfillment of tax and contribution obligations

Pursuant to Section 50 (1) of Act CL of 2017 on the Taxation Procedure, the Enterprise shall submit an electronic declaration every month, by the twelfth day of the month following the month in question, of all taxes, contributions and/or data specified in paragraph (2) related to payments and benefits made to natural persons resulting in tax and/or social security obligations.

The scope of data affected by data processing: the head of the Enterprise, his employees, and their family members.

The scope of data processed: the data specified in Section (2) of Article 50 (2) of the head of the Enterprise, his employees, and their family members, highlighting the natural person's personal identification data (including the previous name and title), gender, citizenship, the tax identification number of the natural person, and the social security identification number.

The recipients are: employees and data processors of the Company performing accounting and payroll activities as part of their job duties.

The Company is entitled to process personal data recorded in the course of fulfilling the legal obligation specified above for 8 years from the termination of the legal relationship.

1.21 Data processing related to the website operated by the Company

1.21.1 Information related to the data of visitors to the Company's website

During visits to the Company's website, one or more cookies - small information packages that the server sends to the browser, and then the browser sends back to the server on each request directed to the server - are sent to the computer of the person visiting the website, through which their browser will be uniquely identified, if the person visiting the website has given their express (active) consent to this by their behaviour of continuing to browse the website after being clearly and unambiguously informed.

About the Users Lake Spirit Kft. In addition, it only collects information (IP address, time of use, website viewed, browser program, and one or more cookies enabling the unique identification of the browser) that it uses exclusively for the development and maintenance of the Service Provider, or for statistical purposes. The service provider uses the data processed for these statistical purposes only in a form unsuitable for personal identification. The cookies used on the website do not store information suitable for personal identification, and the Company does not process personal data in this area. In order to improve the quality of the Services, Solvatory Kft. places a file containing a character string, a so-called cookie, on the User's computer, if the User consents to this.

1.21.2 Data processing related to direct marketing activities

The legal basis for the Company's data processing for direct marketing purposes is the consent of the data subject, which is clear and explicit. The data subject provides his clear, explicit prior consent on paper, by filling out the data form forming Annex 1 to the Data Management and Data Protection Regulations.

After being informed about the processing of your data.

The scope of data subjects: all natural persons who give their clear, express consent to the Company processing their personal data for direct marketing purposes.

The purposes of data processing: maintaining contact with the Company, sending advertisements and offers related to the provision of services and product sales by electronic means or by post.

The recipients of personal data: the manager of the Company, employees performing customer service tasks and marketing tasks based on their job.

The scope of personal data processed: name, address, telephone number, e-mail address.

Duration of data processing: processing of personal data for direct marketing purposes until the data subject withdraws it.

1.21.3 Data processing activities related to the performance of a contract

The Company processes the personal data of natural persons contracting with it - clients, buyers, suppliers - in connection with the contractual relationship. The data subject must be informed about the processing of personal data.

The scope of data subjects: all natural persons who establish a contractual relationship with the Company.

The legal basis for data management is the performance of a contract, the purpose of data management is to maintain contact, enforce claims arising from the contract, and ensure compliance with contractual obligations.

Recipients of personal data: the manager of the Company, the employees of the Company performing customer service and accounting tasks based on their job, and data processors.

The scope of personal data processed: name, address, registered office, telephone number, e-mail address, tax number, bank account number, entrepreneur ID number, primary producer ID number.

Duration of data management: 5 years from the termination of the contract.

2. Data processing rules

2.1 General data processing rules

The Company uses an external data processor entrusted with the personal data it processes to perform the following tasks:

- website operation and maintenance,

- fulfilment of tax and accounting obligations,

- fulfilment of ordered services.

The list of data processors is included in Annex 3 to these regulations.

The rights and obligations of the data processor regarding the processing of personal data are determined by the data controller within the framework of the law and separate laws on data processing.

The Company declares that the data processor does not have the competence to make substantive decisions regarding data processing during its activities, may process the personal data it has obtained only in accordance with the data

controller's instructions, may not process data for its own purposes, and is obliged to store and preserve the personal data in accordance with the data controller's instructions.

The Company is responsible for the legality of the instructions given to the data processor regarding data processing operations.

The Company is obliged to provide information to the data subjects about the identity of the data processor and the place of data processing.

The Company does not authorize the data processor to use another data processor.

The data processing contract must be in writing. Data processing cannot be entrusted to an organization that has an interest in the business activity using the personal data to be processed.

1.21 Data processing activities carried out by the Company

The Company undertakes and provides appropriate guarantees for the compliance of the data processing activities carried out by it as a data processor with the requirements set out in the Regulation and for the implementation of appropriate technical and organizational measures to ensure the protection of the rights of data subjects.

The Company as a data processor shall immediately inform the data controller if it believes that any of its instructions infringe this Regulation or national or EU data protection provisions.

The Company shall process the Data on the instructions of the Data Controller, in accordance with the data protection rules and principles, and shall be obliged to pay attention to the contractual obligations of the Data Controller known to the Data Processor.

The Company may not modify, delete, copy, link the data provided to it by the data controller with other databases, use it for purposes other than this Agreement or for its own purposes, or disclose it to third parties, except to the extent that the Data Controller expressly requires it to do so and it is necessary for the purpose of Data Processing.

The Company is not entitled to represent the Data Controller or to make legal statements on behalf of the Data Controller, unless expressly authorized by an agreement concluded with the Data Controller or another document.

The Company notes that the Data Controller has the exclusive right to determine the purpose and method of processing the data provided to the Data Processor.

The Company, as a data processor, is obliged to ensure the security of the data, to take all technical and organizational measures necessary to enforce the data protection rules, and accordingly, to take measures against unauthorized access to the data, unauthorized alteration, transmission, disclosure, deletion, and destruction of the data. It is also obliged to take appropriate measures against accidental destruction and damage, as well as against inaccessibility resulting from technical changes.

The Company undertakes full obligation to comply with the provisions of this policy regarding data security during its data processing activities, and the provisions set out therein also apply to its data processing activities.

The Company, as a data processor, provides access to the data only to those employees who need it in order to perform the data processing activities, and provides information to those with access about the obligation to comply with security requirements and confidentiality.

The Company, as a data processor, undertakes to cooperate with the data controller in order to enable the data controller to comply with its legal obligations. The cooperation covers in particular the following areas: the fulfillment of requests related to the exercise of the rights of access, deletion and rectification of the data subjects within the legal deadline.

The Company, as a data processor, undertakes to modify, supplement, correct, block or delete the data processed by it in accordance with the instructions of the data controller.

The Company is obliged to notify the data controller immediately of any event or risk affecting the security of the data, to take the measures related to these and to fully cooperate with the data controller.

The Company undertakes to fully cooperate with the data controller and its agents during the inspection and investigation of its systems, records, data, information

and procedures related to data processing. In this context, it ensures that the person authorized to inspect has full access to the records related to data processing, the data files stored in them, and the procedures applied during data processing.

2. Data security provisions

2.1 Principles for implementing data security

The Company may only process personal data in accordance with the activities set out in this policy and in accordance with the purpose of data management.

The Company ensures data security, and in this regard undertakes to take all technical and organizational measures that are essential for the enforcement of data security laws, data and privacy protection rules, and to develop procedural rules necessary for the enforcement of the above-mentioned laws.

The technical and organizational measures to be implemented by the Company are aimed at:

a. encryption of personal data;

b. ensuring the continuous confidentiality, integrity, availability and resilience of systems and services used to process personal data;

c. in the event of a physical or technical incident, the ability to restore access to personal data and the availability of data in a timely manner;

d. the application of a procedure for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures taken to guarantee the security of data processing,

When determining the appropriate level of security, the risks arising from data processing must be expressly taken into account, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized access to personal data transmitted, stored or otherwise processed.

The Company protects the data with appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction and damage, as well as against inaccessibility resulting from changes in the technology used.

The Company records the data it processes in accordance with applicable laws, ensuring that only those employees and other persons acting in the interests of the Company who need to know the data for the purpose of performing their jobs and tasks may access the data.

The Company stores the personal data provided during each data processing activity separately from other data, with the proviso that - in accordance with the above provision - the separated data files may only be accessed by employees with appropriate access rights.

The Company's managers and employees do not transfer personal data to third parties and take the necessary measures to exclude unauthorized access.

The Company grants access to personal data to those employees who have submitted a confidentiality statement regarding the personal data processed to

the obligation to comply with the data security rules. The confidentiality statement is part of the employment contract.

When determining and applying measures for data security, the Company takes into account the current state of technology and, in the case of several possible data processing solutions, chooses the solution that ensures a higher level of protection of personal data, unless it would represent a disproportionate difficulty.

2.2 Protection of the Company's IT records

The Company shall take the following necessary measures to ensure data security with regard to its IT records:

a. It shall provide the data files it manages with permanent protection against computer viruses (it shall use real-time virus protection software).

b. It shall ensure the physical protection of the hardware devices of the IT system, including protection against natural damage,

c. It shall ensure the protection of the IT system against unauthorized access, both in terms of software and hardware devices,

d. It shall take all measures necessary to restore the data files, perform regular backups, and implement separate, secure management of backup copies.

2.3 Protection of the Company's paper records

The Company shall take the necessary measures to protect paper records, in particular with regard to physical security and fire protection.

The Company's manager, employees, and other persons acting in the interest of the Company are obliged to securely store and protect the data carriers they use or possess that contain personal data, regardless of the method of recording the data, against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage.

2. Other provisions

The Company’s CEO is obliged to explain the provisions of this policy to all employees of the Company.

The Company’s CEO is obliged to ensure that all employees of the Company comply with the provisions of this policy. For the purpose of implementing this obligation, the Company’s CEO shall require the amendment of the employment contracts concluded with the Company’s employees in such a way that the employee’s commitment to comply with and enforce this policy is declared.

The establishment and amendment of this policy is within the scope of the Company’s CEO.

3. Scope and review procedure

The Data Processing Policy shall enter into force on May 25, 2018 and shall be valid until revoked. Upon the entry into force of the Data Processing Policy, all previously effective internal regulations or employer instructions, taking into

account which the Company processed personal data under the scope of the Data Processing Policy, shall cease to have effect.

The Data Management Policy shall be reviewed at least once a year, up to and including the effective date of the Data Management Policy, with the review fully covering the content of all annexes. If necessary, the Company shall take appropriate measures to amend the Data Management Policy in accordance with legal and internal organizational changes, ensure the entry into force and publication of the amended Data Management Policy, and ensure that persons falling within the personal scope of the Data Management Policy are informed of the content of the amendments.

It is mandatory for all representatives, officers and agents of the Company to familiarize themselves with and comply with the applicable rules of the Data Management Policy, and they shall perform their duties in full compliance with the provisions of the Data Management Policy.

In the event of a change in legislation or in the event of a modification of this regulation for other reasons, the Information must be modified based on the change in legislation or for other reasons and the text of the modification must be explained to the Data Subjects.

The Data Management Regulation contains the following annexes:

Annex 1 Declaration of consent to data processing

Annex 2 Consent to data processing for DM purposes

Annex 3 Register of data processors

Annex 4 Extracts from Regulation (EU) 2016_679 of the European Parliament and of the Council, Articles 13 and 14

Annex 5 Register of data processing

Annex 6.1 Data processing information for employees

Annex 6.2 Website data processing information

Annex 7.1 CV information for job applicants

Annex 7.2 CV information for non-job applicants

Annex 8.1 Annex 8.2. Data Protection Incident Registration

Annex 8.2. Data Protection Incident Notification

Budapest, September 1, 2023

_____

Lake Spirit Kft.