







may be rejected

- for the exercising of the right to freedom of expression and information, or
- when processing of personal data is allowed by law; and
- for the submission, enforcement or defence of legal claims.

In any event, the Company shall inform the Data Subject of the refusal of a request for erasure, indicating the reason for the refusal. Once a request for erasure of personal data has been fulfilled, previous (erased) data can no longer be recovered.

#### **9.4. Right to restriction of processing:**

The Data Subject shall have the right to obtain from the Controller restriction of processing if the accuracy of the personal data is contested by the Data Subject. In such a case, the restriction shall apply to a period enabling the Company to verify the accuracy of the personal data. The Company shall identify the personal data it processes if the Data Subject contests its correctness or accuracy, but the inaccuracy of the personal data in dispute cannot be clearly established. In addition, the Data Subject may request that the processing of his or her personal data be restricted by the Controller if the purpose of the processing has been fulfilled, but the Data Subject requires its processing by the Controller for the submission, validation or defence of legal claims.

#### **9.5. Right to object:**

The Data Subject may object to the processing of his / her personal data,

- if the processing is necessary only to fulfil the legal obligation of the Controller or to enforce the legitimate interest of the Controller or a third party;
- if the purpose of the processing is direct marketing, public opinion polling or scientific research; or
- if the processing has become necessary for the performance of a task carried out for reasons of public interest.

The Controller shall examine the lawfulness of the Data Subject's objection and, if it is established that the protest is well founded, the Controller shall suspend processing, block the personal data processed and inform those to whom the personal data have previously been transmitted.

#### **9.6. Right to withdraw consent:**

The Data Subject has the right to withdraw his/her consent to the processing of personal data processed with his/her consent at any time. The withdrawal shall not affect the lawfulness of the processing of personal data prior to the withdrawal of the consent. The consent can be withdrawn via e-mail sent to address [info@xxxxxx.com](mailto:info@xxxxxx.com).

#### **9.7. Right to data portability:**

The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Controller, either in printed form or in a structured, commonly used and machine-readable format (XML/XLS/CSV) and the personal data shall be transmitted – if requested by Data Subject - to another controller by the Company.

### **10. Security of personal data:**

For protection of personal data, the Company has taken and applied the following data security measures:

### **10.1. Physical security**

In the company seat there is an electronic access system and reception service operating. The Company has a camera system at its seat and place of business to protect against unauthorized or violent intrusion, fire or natural disaster. Paper-based personal information is stored in a locked place that is accessible only to authorized persons.

### **10.2. Data security in the IT infrastructure**

Personal data are stored on servers provided by the hosting service provider, which is subject to very limited personal and employee access under strict permission and management rules. We test and verify our IT systems periodically and regularly to ensure and maintain data- and IT security. Office workstations are password protected, use of external media is controlled and only allowed under secure conditions after verification. All of our systems and components are protected against systemic and ongoing malicious software. When designing, developing, testing and operating programs, applications, and tools, we prioritize security features separately.

### **10.3. Data security in communications**

In order to meet the requirements of secure data exchange for messages and files transmitted electronically, we ensure data integrity for both (communication) control and user data. Error detection and correction procedures are used to prevent data loss and damage. For applications, passwords, permissions, and other security-related parameters and data can only be transmitted encrypted. We prevent and eliminate data loss and damage through error detection and correction procedures and ensure that they are not denied. In the case of a data transmission network, we ensure that illegal connections and eavesdropping are prevented in a manner appropriate to the level of security.

### **10.4. Data security during document management**

We also satisfy the data security requirements set out in our records policy. The records are handled in accordance with written authorization levels and in accordance with the security rules applicable to each document's confidentiality. We have detailed and strict rules regarding the destruction, storage and issue of documents.

## **11. Measures to be taken in the case of data protection breach**

Any possibly arising data protection breaches shall be reported to the supervisory authority in compliance with laws within 72 hours, and we shall keep records on data protection breaches. In the cases specified by law, we shall also inform the data subjects of the breach.

## **12. Duration of processing**

We shall retain the personal data contained in the contracts concluded with clients for a period of 5 years.

For the compliance with accounting and tax regulations, personal information in this respect shall be retained for seven years after the tax year ended.

We shall retain the documentation related to the employment relationship for 4 years following the termination thereof.

Personal information you provide when signing up for the newsletter will be retained for 3 years.

### 13. Legal remedies

Data Subjects may contact the Company by using the following contact details if they have any question or observation: e-mail: [info@lugos-reneables.com](mailto:info@lugos-reneables.com), telephone number: +36-30-586-6854.

The Data Subject may lodge their complaint related to processing pursued by the Company directly to the Hungarian National Authority for Data Protection and Freedom of Information (address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.; telephone: +36-1-391-1400; e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); website: [www.naih.hu](http://www.naih.hu)).

In the case of any violation of the rights of the Data Subject, he or she may seek remedy at the court. The court with jurisdiction to settle the case shall be the regional court. At the choice of the Data Subject, the lawsuit may be instituted before the court in the place where the data subject is domiciled or habitually resident. Upon request, the Controller shall inform the User of the possibility and means of redress.

### 14. For the purposes of this notice:

14.1. **'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;

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

14.3. **'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;

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

14.5. **'consent of the data subject'** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

14.6. **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Baja, 20.11.2020.

**LUGOS Renewables Kft.**