

## PRIVACY AND DATA PROTECTION NOTICE

### Optimum Solar Schedule and Storage LTD.

Effective date: 03.05.2022.

**Optimum Solar Schedule and Storage LTD.** (registered office: 6500 Baja, Gesztenye street 2., company registration number: 03 09 132685, tax number: 26729879-2-03, represented by: István Halász, e-mail: info@optimumsss.com, telephone: +36 30 629 5197, hereinafter the Company) provides the following information in accordance with Regulation 2016/679 of the European Parliament and of the Council on the General Data Protection Regulation (hereinafter: GDPR) in relation to its data processing activities.

#### 1. Our data processing activities:

The Company acts as a data controller in relation to personal data relating to the following activities:

- 1.1. receiving requests for quotations from customers, making quotations, concluding contracts and processing personal data relating to the performance of contracts
- 1.2. liaising for the purpose of marketing activities; recording partner data for enhancing the business and marketing strategies and organizing business events,
- 1.3. debt management;
- 1.4. assertion of legitimate interests.

#### 2. Our data processing activities by purpose:

Description of processing and purpose	Legal basis for processing	Type of data processed and their source	Duration of processing	Data processor
<b>Receiving requests for proposals from clients, submitting proposals, concluding contracts, maintaining contractual relations.</b>	<b>Performance of the contract pursuant to Article 6(1)(b) of the GDPR</b>	For natural persons: name, address, tax identification code, telephone number, e-mail address, fax number, billing address.  For legal entities: contact name, e-mail address, telephone number.  Source of data: natural person: directly from the data subject Legal entity: directly from the data subject, or from their employer	5 years from the termination of the contractual relationship with the client in connection with the enforcement of a civil claim or the performance of an obligation (Act V of 2013 on the Civil Code ("Civil Code") Section 6.22 (1)).  Billing-related data processing:  In the case of tax documents: 5 years from the last day of the calendar year in which the relevant tax should have been declared,	Pálkerti Adótanácsadó és Könyvelő Kft.(accounting services)  NETCLASS Kft. (IT services)

			<p>reported or notified, or in the absence of a declaration, reporting or notification, the tax should have been paid (Act CL of 2017 on the Rules of Taxation, Section 78 (3) and Section 202 (1)).</p> <p>For accounting documents: 8 years (Act C of 2000 on Accounting, Sections 168-169).</p>	
<p><b>Liaising for the purpose of marketing activities; recording partner data for enhancing the business and marketing strategies and organizing business events</b></p>	<p><b>Consent given by the data subject as per Article 6 (1)a) of the GDPR</b></p>	<p>First name, last name, e-mail address, telephone number, title and position.</p>	<p>Data will be processed until the partnership is maintained, but at the latest until the withdrawal of the data subject's consent.</p>	<p><b>Netclass Kft.</b> IT services</p>
<p><b>Payment reminders, debt management</b></p>	<p><b>Article 6(1)(f) of the GDPR (processing is necessary for the purposes of the Company's legitimate interests).</b> Legitimate interest: processing for the purpose of recovering any outstanding debt owed to the Company by the Client following the use of any design and development services</p>	<p>User name, surname, first name, e-mail address and home address</p> <p>Source of data: from the Company's internal database (contracts, orders, customer service data)</p>	<p>In the event of a demand for payment by the Company: for <b>5 years</b> from the termination of the contract.</p> <p>In case of enforcement proceedings: <b>5 years from the closure of the debt management case.</b></p>	
<p><b>Assertion of legitimate interests</b></p> <p>Retention of data relating to the Company's communications with Customers and other data</p>	<p><b>Article 6(1)(f) of the GDPR (processing is necessary for the purposes of the Company's legitimate interests).</b> Legitimate interest: the assertion of a claim by the</p>	<p>User name, surname, first name, e-mail address, contractual data, bank account number, other data necessary for exercising legal claims or for the</p>	<p>The Company shall retain documents (e.g. e-mails, letters, paper requests) and other requests related to communications provided by the Company and its Customer Service for <b>5 years</b> after their receipt</p>	<p><b>Net-Class Kft.</b> (1139 Budapest, Fáy street 1/b. I. floor 2. office)  IT service provider</p>

<p>subjects for the purposes of pursuing legal claims and successfully defending any legal dispute or legal proceedings.</p>	<p>Company and the successful defence of a legal dispute or legal proceeding brought by the Customer.</p>	<p>defence of legal proceedings (for example: data voluntarily provided by the data subject when contacting the client at the first time).</p> <p>Source of data: Internal database of the Company.</p>	<p>(in case of e-mails, when they become available, in case of telephone calls, when they are recorded) by the Company or the Customer Service (in accordance with section 6:22 (1) of the Civil Code. 6:22 (1)), with a view to the enforcement of any civil claims made by the Company and for the defence against any civil claims submitted by the data subject.</p> <p>Where the processing of personal data is necessary for the defence of a judicial or administrative procedure initiated by the data subject or for the purposes of the pursuit of legitimate interests pursued by the Company, the Company is entitled, on the basis of its legitimate interests (Article 6(1)(f) of the GDPR), to process the personal data concerned until the final conclusion of such procedure or until the pursuit of the legitimate interests by other means (e.g. the conclusion of an out-of-court settlement), and where it is not necessary to keep a complete written or electronic document containing the data, the right to extract the data from that document according to the scope of the data required.</p>	
--	---	---	--	--

### **3. Sub-controllers:**

The Company, in accordance with Article 6(1)(f) of the GDPR (on the basis of the Company's legitimate interest), uses the services of its legal partners for the management and successful enforcement of its outstanding claims - and transfers to them the personal data necessary for this purpose (including in particular: the data of its contractual partners, their contact persons, data indicated in the contract of representation, data related to any claims) – and such partners will act as independent data controllers as set out in their respective privacy notices. At the request of the data subject, the Company shall provide information on the legal partners used for such specific processing, their contact details, the activities carried out by them, and the data processed in the context of such activities.

### **4. Name, registered office, telephone number, website (where privacy notices are available) and e-mail address of data processors:**

Netclass Kft., IT services, contact information: 6353 Dusnok, Táncsics Mihály street 11., telephone: +36 30 224 5650; e-mail: [info@netclass.eu](mailto:info@netclass.eu), web: [www.netclass.eu](http://www.netclass.eu).

Pálkerti Adótanácsadó és Könyvelő LTD., accounting services; contact information: 6500, Baja Czirfusz Ferenc street 7.; telephone: +36 20 969 5611; e-mail: [konyveles@palkerti.hu](mailto:konyveles@palkerti.hu); website: [www.palkerti.hu](http://www.palkerti.hu)

#### **Data Transfer:**

The names, addresses, telephone numbers and e-mail addresses of the customers will be provided to the contractors engaged by the company for the performance of contracts, and for the construction and implementation works of the power plant.

To fulfil its statutory obligations, the company will forward the buyer and seller data, invoice items and invoice details contained in its invoices to the National Tax and Customs Administration.

In the event of a request from a public authority (e.g. the Consumer Protection Authority, the National Authority for Data Protection and Freedom of Information), personal data of customers may be transferred within the scope and to the extent specified in such request.

The Data Controller shall ensure the security of personal data, take technical and organisational measures and establish procedural rules to ensure that the personal data recorded, stored or processed are protected and to prevent their accidental loss, unlawful destruction, unauthorised access, unauthorised use, unauthorised alteration or unauthorised disclosure. To fulfil this obligation, the Data Controller will call all third parties to whom it transfers personal data to.

In view of the relevant provisions of the GDPR, the Data Controller is not obliged to appoint a Data Protection Officer.

### **5. Access to personal data by company employees:**

The company will ensure that the company's customer-facing employees have access to the personal data it processes and only to the extent strictly necessary for the performance of their work. All access to data will be logged and only the IT operator has access to the data recovery function.

The data backup operations are carried out by the Data Controller through the Data Processor using encryption, so that in the event of any data recovery, employees will not have access to the backed-up personal data.

Employees of the Company do not have access to servers containing sensitive data.

### **6. The rights of the data subject in relation to the processing of their personal data:**

Your data protection rights and remedies and their limitations are set out in detail in the GDPR (in particular Articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79 and 82). You may request information about your data at any time, i.e. you may request the rectification, erasure or restriction of the processing of your data, or may object to their processing based on legitimate interest.

#### **6.1. Right of access:**

The Data Subject may request that the Company inform them whether the Company processes their personal data and, if so, provide them with access to the personal data processed by the Company. The Data Subject may request information about the processing of personal data at any time by sending a written request by registered or certified mail to the Company's address or by e-mail to [info@optimumsss.com](mailto:info@optimumsss.com). The Company will consider a request for information sent by letter as authentic if the Data Subject can be clearly identified on the basis of the request sent. The Company will only consider a request for information sent by e-mail to be authentic if it is sent from the e-mail address provided by the Data Subject to the Company, but this does not preclude the Company from identifying the Data Subject in another way before providing the information.

The request for information may cover the data of the Data Subject processed by the Company, the source of such data, the purpose of processing, the legal basis and duration of the processing, the names and addresses of any Data Processors and the activities related to the processing.

#### **6.2. Right to rectification:**

The Data Subject may request the correction, clarification or modification of their personal data processed by the Company. Taking into account the purpose of the processing, the Data Subject may request the completion of incomplete personal data. Once a request to amend personal data has been fulfilled, the previous (deleted) data can no longer be restored.

#### **6.3. Right to erasure:**

The Data Subject may request the erasure of personal data processed by the Company. Erasure may be refused

- for the purpose of exercising the right to freedom of expression and information, or
- if the processing of personal data is permitted by law; and
- for establishing, exercising or defending of legal claims.

In all cases, the Company shall inform the Data Subject of the refusal of the request for erasure, indicating the reasons for the refusal. Once a request for erasure of personal data has been fulfilled, the previous (erased) data can no longer be restored.

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

The Data Subject may request that the controller restricts the processing of their personal data if the Data Subject contests the accuracy of the personal data processed. In this case, the restriction applies for the period of time that allows the Company to verify the accuracy of the personal data. The Company shall mark the personal data it processes if the Data Subject contests the accuracy or correctness of the personal data, but the inaccuracy or incorrectness of the contested personal data cannot be clearly established. The Data Subject may also request that the Data Controller restrict the processing of their personal data where the purpose of the processing has been achieved, but the Data Subject requires the Data Controller to process the data for the establishment, exercise or defence of any legal claim.

#### **6.5. Right to object:**

The Data Subject may object to the processing of their personal data,

- where the processing of personal data is necessary for the purposes of the legitimate interests pursued by the Data Controller or a third party;
- if the purpose of the processing is direct marketing, public opinion polling or scientific research; or
- if the processing is carried out for the performance of a task carried out in the public interest.

The Data Controller shall examine the lawfulness of the Data Subject's objection and, if the objection is justified, shall terminate the processing and block the personal data processed, and shall notify the objection and the action taken on the basis thereof to all those to whom the personal data concerned by the objection have been disclosed in the past.

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

The Data Subject has the right to withdraw their consent to the processing of personal data processed with their consent at any time. The withdrawal does not affect the lawfulness of the processing prior to the withdrawal of consent. Their consent may be withdrawn in an e-mail sent to [info@optimumsss.com](mailto:info@optimumsss.com).

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

The Data Subject may request that the personal data provided by them be transferred to us either on paper or in a structured, commonly used, machine-readable format (XML/XLS/CSV) and/or, at the Data Subject's request, to another controller, by the Data Controller.

### **7. Data security:**

The Company has implemented and applies the following information security measures to protect data:

#### **7.1. Physical security**

The registered office has an electronic access system and a reception desk. The Company's headquarters and premises are equipped with a camera system to provide security against unauthorised or forced entry, fire or natural disasters. Personal data processed on a paper basis is stored in a locked cabinet, accessible only by those authorised to access it.

#### **7.2. Data security in IT infrastructure**

The personal data is stored on servers provided by the hosting provider, to which only a very limited number of staff and employees have access, based on strict access control rules. IT systems are tested and audited on a recurring and regular basis to establish and maintain data and IT security. Office workstations are password-protected, and the use of foreign media is regulated and only allowed under secure conditions and after verification. Regular and continuous protection against malware is provided for all our systems and components. We prioritise and separate security functions in the design, development, testing and operation of programs, applications and tools.

#### **7.3. Data security in communications**

To meet the requirement of secure data exchange for electronically transmitted messages and files, we ensure data integrity for both (communication) control and user data. We apply error detection and correction procedures to avoid data loss and corruption. In the case of applications, any passwords, privileges and other security-related parameters and data may only be transmitted in encrypted form. We prevent data loss and corruption through error detection and remediation procedures and ensure non-repudiation. For the network used for data transmission, we will ensure that illegal connections and eavesdropping are prevented in a manner appropriate to the level of security.

#### **7.4. Data security in document management**

We also comply with the requirements of data security in the management of documents, which we have laid down in our document management policy. We handle documents according to written authorisation levels and

security standards appropriate to the confidential nature of each document. We have detailed and strict rules on the destruction, storage and disclosure of documents.

## 8. Measures to be take in the event of data breach

We report any data protection incidents to the supervisory authority in accordance with the law within 72 hours of becoming aware of the data protection incident and keep records of data protection incidents. In cases specified by law, we also inform the data subjects about the incident.

## 9. Enforcement options

If you have any questions or comments regarding data processing, please contact the Company at the following contact details: via e-mail [info@optimumsss.com](mailto:info@optimumsss.com) and by telephone: +36 30 629 5197.

The Data Subject may refer directly to the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa street 9-11; telephone: +36-1-391-1400; e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); website: [www.naih.hu](http://www.naih.hu)) about any complaint regarding the data processing carried out by the Company.

In the event of a breach of the Data Subject's rights, the Data Subject may take legal action. The court of law has jurisdiction to hear the case. The action may also be brought before the court of the person's domicile or residence, at the discretion of the person concerned. At the request of the Data Controller, the User shall be informed of the possibilities and means of redress.

## 10. Definitions used in the Notice:

**10.1 "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;

**10.2 "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;

**10.3 "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;

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

**10.5 "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;

**10.6 "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.

**Optimum Solar Schedule and Storage LTD.**