PRIVACY POLICY

Date of effect: 29.08.2022

The **Optimum Solar Zártkörűen Működő Részvénytársaság** (hereinafter the „OS Zrt." or the „Company") registered seat: 1123 Budapest, Alkotás utca 53. A. ép. 6. em.; registered at Budapest-Capital Regional Court; registration number: Cg. 01 10 141967; tax number: 27193932-2-43, e-mail: info@optimumsolar.eu, phone: +36 1 808 9480) provides the following information in accordance with Regulation No. 2016/679 of the European Parliament and Council on the General Data Protection Regulation (hereinafter: GDPR[1]) on its data processing activities.

1. Data Processing activities:

The Company acts as a data controller in case of the following activities:

1.1. receiving requests for quotations from customers, submitting offers, concluding contracts and processing personal data relating to the performance of contracts

1.2. maintaining contact in connection with marketing activities; recording partner data for the purposes of business strategy, marketing strategy, business events,

1.3. Depth recovery and receivables management;

1.4. legal representation.

2. Our data processing activities by purpose:

Description and the purpose of the processing	**Legal basis of the processing**	**Scope of the processed data and their source**	**Period of data processing**	**Data processor and its activity**
Receiving requests for proposals from clients and contractors, submitting offers, concluding contracts and maintaining contractual relations.	Performance of the contract for an natural person or sole proprietor based on Article 6 (1) b) In case of legal person (entity) data processing is based on Article 6 (1) (f) of the GDPR , the data processing is also necessary for the purposes of the legitimate interests	For natural person and sole proprietors: name, address, tax identification number, telephone number, e-mail address, fax number, billing address. For legal persons, contact name, e-mail address, telephone number. Source of data in case of natural person: directly from the data subject; In case of legal person: directly from the data subject or the data subject's Employer	Regarding the exercise of any potential civil law claims of the Company or to defend against any potential civil law claims of the data subjects, the Company process the personal data for 5 years (pursuant to Section 6:22 (1) of Act V of 2013 on the Civil Code ("Civil Code"), from the termination of the contract. Regarding the invoicing: In the case of tax documents: 5 years from the last day of the	Pálkerti Könyvelő Iroda Kft. (accounting service) (6500 Baja, Czirfusz Ferenc u. 7. konyveles@palkerti.hu) RSM Audit Hungary Zrt. (financial auditor) (1139 Bp, Váci út 99-105. Balance Hall. ép. 4. em rsm.audit@rsm.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

			calendar year in which the tax return, data declaration, or notification should have been made, or in the absence of a return, data declaration, or notification, the tax should have been paid (Act CL of 2017 on the Rules of Taxation. § 78 (3), § 202 (1)). In the case of accounting documents: 8 years (§ 168-169 of Act C of 2000 on Accounting).	hu) NETCLASS Kft. (IT szolgáltatás) 1139 Budapest, Fáy utca 1/b. info@netclass.eu IT supporting Kulcs-Soft Nyrt. (software providers) (Budapest, Mészáros u. 13, 1016)
Data processing related to marketing, business strategy, marketing strategy, business events	**Consent of the data subject pursuant to Article 6(1)(a) of the GDPR**	First name, last name, e-mail address, telephone number, title, position.	The data will be processed until the partnership is terminated, but at the latest until the data subject's consent is withdrawn.	**NETCLASS Kft.** IT services
Payment reminders, Debt management	**Article 6(1)(f) GDPR** (processing is necessary for the purposes of the legitimate interests pursued by the Company). Legitimate interest: processing for the purpose of recovering unpaid debts owed to the Company by the Client following the use of a design and development service.	first name, last name, e-mail address, mobile number, in case of natural person: home address Data source: from the Company's internal database (contracts, orders, customer service data)	In the event of a demand for payment by the Company: **for 5 years from the termination of the contract.** In the event of enforcement proceedings being initiated: **5 years from the closure of the debt collection case.**	
Enforcement of legal claims Data processing related to the Company's communications with Customers, courts and other	**Article 6(1)(f) GDPR** (processing is necessary for the purposes of the legitimate interests pursued by the Company). Legitimate interest:	Last name, first name, e-mail address, data included in the contract, bank account number, other data necessary for asserting legal	The Company archive the documents related to the communication between the data subject and employee of the Company, Customer Service etc. (for example: e-mails, letters, paper-based	

data subjects for the purposes of pursuing legal claims and successfully defending a dispute or legal action.	the pursuit of claims by the Company and the successful defence of a dispute or legal action brought by the Customer.	claims and defense in court or official proceedings (for example: data voluntarily provided by the data subject in the given request). Data source: Company's internal database.	inquiries) and other inquiries for 5 years after their receipt by the Company (in the case of e-mails they become accessible according to § 6:22. (1) of the Civil Code), with regard to the enforcement of the Company's possible civil rights claims, as well as the defense against the possible civil rights claims of the person concerned. If the processing of personal data is necessary for defense in court or official proceedings initiated by the data subject or for the enforcement of the legitimate interests of the Company, the Company is entitled to process the relevant personal data on the basis of its own legitimate interests (GDPR Article 6 (1) point f) until completion or until the legitimate interest is asserted by other means (e.g. conclusion of an out-of-court agreement), and - if it is not necessary to preserve the entire written or electronic document recording the data - you are entitled to prepare an extract from the given document according to the scope of the necessary data.	

3. **Other data controllers:**

The Company uses the services of its legal partners for the processing and successful enforcement of its outstanding litigation and non-contentious claims and claims pursuant to Article 6(1)(f) of the GDPR (based on the Company's legitimate interest). Company also transfers to them the personal data necessary for this purpose (including in particular: data of its contractual partners, their contact persons, data indicated in the contract of representation, data of claims). These legal partners 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 partner acting in relation to a specific processing operation, the contact details of the legal partner, the activity carried out by the legal partner and the scope of the data processed in the context of that activity.

4. **Name, address, telephone number, website (where data protection information is available) and e-mail address of data processors**

NETCLASS Kft. information technology and support (Availability: seat at 6353 Dusnok, Táncsics Mihály str. 11. phone: +36 30 224 5650; e-mail: info@netclass.eu web: https://www.netclass.eu/)

Pálkerti Könyvelő Iroda Kft. accounting and bookkeeping activities (Availability: seat at Baja, Czirfusz Ferenc u. 7.; e-mail: konyveles@palkerti.hu)

RSM Audit Hungary Zrt. auditor (Availability: seat at 1139 Budapest, Váci út 99-105. Balance Hall. building. 4. floor; phone: (06 1) 886 3700; e-mail: rsm.audit@rsm.hu)

Kulcs-Soft Nyrt.: software supporting (Availability: seat at 1016 Budapest, Mészáros str. 13. phone: +36 1 336 5300 info@kulcs-soft.hu)

5. **Transfer of personal data**:

The names, addresses, telephone numbers and e-mail addresses of the customers, business partners will be provided to the contractors and subcontractors of the Company for the purpose of the performance of the contract, construction and implementation of the power plant or other written contractual purpose and obligation.

Based on statutory obligations the Company shall transfer personal data, invoice items and invoice details contained in its invoices to the National Tax and Customs Administration (NAV).

In the event of a request by a public authority (e.g. the Hungarian Energy and Public Utility Regulatory Office (MEKH), the Consumer Protection Authority, the National Authority for Data Protection and Freedom of Information (NAIH)), the personal data of customers, business partners may be transferred within the scope and to the extent specified in the request by the public authority.

The Company does not transfer personal data to third countries not party to the GDPR regulation, but only to the data processors named in this information notice and to the categories of addressees listed herein for the sole purpose indicated.

The controller and the processor implement appropriate 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. The Data Controller shall draw attention of all third parties to whom it transfers personal data to comply with this obligation.
In view of the relevant provisions of the GDPR, the Data Controller is not obliged to appoint a Data Protection Officer.

6. **The Company's employees' access to personal data:**

In order to provide the service, the Company provides its employees who are involved in the case and the performance of the contract/business contact with the access absolutely necessary for their work only to the personal data managed by them. All access is logged, and only the IT operator has access to the data backup function.

Data backup operations are carried out by encryption by the Data Manager through the Data Processor, so in case of possible data recovery, employees will not have access to the saved personal data.
Company employees do not have access to servers containing live data.

7. The Data Subject's rights regarding the management of his/her personal data:

Your data protection rights and legal remedies and their limitations are detailed in the GDPR (in particular, GDPR Articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79. and Articles 82). You can request information about your data at any time, you can request the correction, deletion or restriction of your data at any time, or you can object to data processing based on legitimate interests.

7.1. Right of access:

The Data Subject may request that the Company informs whether it process the Data Subject's personal data and, if so, to provide her/him with access to the personal data it processes. The Data Subject may request information on the processing of personal data at any time in writing, by registered or registered letter sent to the address of the Company, or by e-mail sent to the e-mail address (info@optimumsolar.eu). The Company considers a request for information sent by letter to be authentic if the Data Subject can be clearly identified based on the sent request. The Company considers a request for information sent by e-mail as authentic only 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 other ways before providing the information.

The request for information may cover the Data Subject's data managed by the Company, their source, the purpose, legal basis, duration of the given data processing, name and address of possible Data Processors, activities related to the data processing.

7.2. Right to rectification:

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

7.3. Right to erasure:

The Data Subject may request the deletion of personal data managed by the Company. Deletion can be refused

- for the purpose of exercising the right to freedom of expression and information, or
- if the law authorizes the processing of personal data; as well as
- to present, enforce and defend legal claims.

In all cases, the Company informs the Data Subject of the refusal of the deletion request, specifying the reason for the refusal of deletion. After fulfilling the request to delete personal data, the previous (deleted) data can no longer be restored.

7.4. Right to restrict data processing:

The Data Subject may request that the processing of his/her personal data be restricted by the data controller if the

Data Subject disputes the accuracy of the processed personal data. In this case, the limitation applies to the period that allows the Company to verify the accuracy of the personal data. The Company marks the personal data it manages if the Data Subject disputes its correctness or accuracy, but the incorrectness or inaccuracy of the disputed personal data cannot be clearly established. Furthermore, the Data Subject may also request that the Data Controller limit the processing of their personal data, if the purpose of the data processing has been achieved, but the Data Subject requires their processing by the Data Controller for the presentation, enforcement or defense of legal claims.

7.5. Right to protest:

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

- if the processing of Personal Data is necessary to enforce the legitimate interests of the Data Controller or a third party;
- if the purpose of data processing is direct business acquisition, public opinion polls or scientific research; obsession
- if the data processing takes place in order to fulfill a task in the public interest.

The Data Controller examines the legality of the Data Subject's objection, and if it finds that the objection is well-founded, it terminates the data management and locks the processed personal data, and notifies all those to whom the personal data affected by the objection were previously transmitted about the objection and the measures taken based on it.

7.6. Right to withdraw consent:

The Data Subject has the right to withdraw his consent to the processing of personal data processed with his consent at any time. The revocation does not affect the legality of data management prior to the revocation of consent. You can withdraw your consent by sending an email to info@optimumsolar.eu.

7.7. The right to data portability:

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

8. Data security:

In order to protect data, the following information security measures have been implemented and are being applied at the Company:

8.1. Physical security

There is an electronic access control system and concierge service at the headquarter. A camera system operates at the Company's headquarters and premises, providing security against unauthorized or forced entry, fire or natural disasters. Personal data handled on a paper basis are stored in a closed place, which can only be accessed by those with access rights.

8.2. Data security in the IT infrastructure

Personal data is stored on servers provided by the hosting provider, which can only be accessed by a very limited

number of employees based on strict authorization management rules. IT systems are repeatedly and regularly tested and checked in order to create and maintain data and IT security. The office workstations are password protected, the use of foreign data carriers is permitted only under controlled and safe conditions, after verification. Regular and continuous protection against malicious software covering all our systems and system components is provided. During the planning, development, testing, and operation of programs, applications, and devices, security functions are handled separately and prioritized.

8.3. Data security in communication

In order to fulfill the requirement of secure data exchange with regard to messages and files transmitted electronically, we ensure the integrity of the data for both (communication) control and user data. In order to avoid data loss and damage, we use error detection and repair procedures. Regarding applications, passwords, authorizations and other security-related parameters and data can only be transmitted encrypted. We prevent data loss and damage with error detection and repair procedures and ensure non-repudiation. In the case of the network used for data transmission, we ensure the prevention of illegal connection and eavesdropping in accordance with the security level.

8.4 Data security during document management

We also comply with the requirements of data security during document management, which we set out in the document management regulations. Document management is carried out according to the authorization levels defined in writing, and according to the security regulations applied in accordance with the confidential nature of each document. We have detailed and strict rules regarding the destruction, storage and issuance of documents.

8.5 Measures in the event of a data protection incident

Any data protection incidents that may arise are reported to the supervisory authority within 72 hours of becoming aware of the data protection incident in accordance with the law, and we also keep records of the data protection incidents. In cases specified by law, we also inform the affected parties about the incident.

9. Legal enforcement options

The Data Subject can file a complaint about the Company's data management directly with the National Data Protection and Freedom of Information Authority (address: 1055 Budapest, Falk Miksa utca 9-11; telephone: +36-1-391-1400; e-mail/address: ugyfelszolgalat@naih .hu; 1363 Budapest, Pf.: 9. website: www.naih.hu).
In the event of a violation of the Data Subject's rights, he may go to court. Adjudication of the lawsuit falls within the jurisdiction of the court. At the choice of the data subject, the lawsuit can also be initiated before the court of the data subject's place of residence or residence. Upon request from the Data Controller, the User will be informed of the possibility and means of legal redress.

10. Terms used in this Privacy Policy:

"personal data": any information relating to an identified or identifiable natural person ("data subject"); a natural person can be identified directly or indirectly, in particular on the basis of an identifier such as name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person identifiable;
"data management": any operation or set of operations performed on personal data or data files in an automated or non-automated manner, such as collection, recording, organization, segmentation, storage, transformation or change, query, insight, use, communication, transmission, distribution or other by making it available, coordinating or connecting, limiting, deleting or destroying;
"data controller": the natural or legal person, public authority, agency or any other body that determines the purposes and means of processing personal data independently or together with others; if the purposes and

means of data management are determined by EU or member state law, the data controller or the special aspects regarding the designation of the data controller may also be determined by EU or member state law;
"data processor": the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller;
"consent of the data subject": the voluntary, specific and well-informed and clear declaration of the will of the data subject, with which the data subject indicates through a statement or an act clearly expressing the confirmation that he gives his consent to the processing of personal data concerning him;
"data protection incident": a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise handled.

Optimum Solar Zrt.