



ITH0023.2 – ITHACA Clean Energy Privacy Notice V1.2 06.06.23

This Notice and Your right to privacy

We understand the importance of your right to privacy. That's why we take the protection of your information seriously and have implemented policies and processes to ensure its security.

This notice outlines the information we may collect from you when you download, install, register with, access, or use the Waterfront mobile app and/or website. It also explains how we collect, use, maintain, protect, and disclose your information.

This notice only pertains to the information we gather via the Platform and electronic communications related to it, such as email and text. It does not cover information collected through other Company apps or websites or by third parties.

We advise you to read the privacy policies of our other websites, apps, and third-party partners before sharing any information with them.

If you disagree with our policies and practices, please refrain from downloading, registering, or using our platform.

We may update this policy from time to time. If you continue using the Platform after we make changes, you agree to the revised policy. To stay informed, please check the policy periodically for updates.

Who we are

We are Ithaca Clean Energy, and you can find out more about us on our website at www.ithacacleanenergy.com.

Because we are based outside the United Kingdom / European Union, we have appointed Data Rep Service office as our local representative.

Our Data Privacy Officer is appointed on a service basis by Data Rep Service Ltd, and if you have any queries or concerns, you can contact them by telephone at +44 (0)1332 720 078 or by email to ithacacleanenergy@datarepservice.com.

How we follow data protection regulations

Our top priority is to protect your personal information and use it ethically. We strictly adhere to all laws related to personal information security. We have implemented various policies and processes to safeguard your personal information to the best of our ability.

The lawful bases that we rely on for processing your information are:

- Your consent, which you can remove at any time.
- We have a contractual obligation.
- We have a legal obligation.
- We have a vital interest.
- We need it to perform a public task; or
- We have a legitimate interest.

We may also monitor and keep records of email communications you send to us and other communications with you per this policy and our other business interests.

Information we use about you

When you enquire about or use our services, we collect personal information about you.

In general, we may use your information to:

- Communicate with you.
- Keep our records up to date.
- Process payments.
- Ensure the safety of users.
- For research and statistical purposes.
- To fulfil our legal and regulatory obligations.
- Process job applications.
- Gain feedback from you.
- Prevent crime and meet our legal obligations.
- Prudentially manage our business using models and forecasts.
- Keep you informed of products or services that may interest you where you have given us consent for us to do so.

We may also collect the following personal information:

- Identifiers, such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
- Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), such as a name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.
- Geolocation data, such as physical location or movements.
- Sensory data, such as audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information, such as a current or past job history or performance evaluations.

We don't collect or use:

- Special Category Information, such as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data; biometric data (where used for identification purposes), data concerning health; data concerning a person's sex life, and data concerning a person's sexual orientation.
- Protected classification characteristics under California or federal law, such as Age (40 years or older), race, colour, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).
- Commercial information, such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information, such as genetic, physiological, behavioural, and biological characteristics or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.
- Internet or other similar network activity, such as browsing history, search history, and information on a consumer's interaction with a website, application, or advertisement.
- Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)), such as education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.
- Inferences drawn from other personal information, such as profile, reflecting a person's preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes.

How we use your information

We use information that we collect about you or that you provide to us, including any personal information, to:

- Provide you with the Platform and its services and any other information, products or services you request from us.
- Fulfil any other purpose for which you provide it.
- Give you notices about your account, including expiration and renewal notices.
- Carry out our obligations and enforce our rights arising from any contracts between you and us, including for billing and collection.
- Notify you when Platform updates are available and of changes to any products or services we offer or provide through it.
- To provide services to you and fulfil the agreement between us.
- To prevent and detect fraud against you or your company.
- To conduct checks to identify our customers and verify their identity.
- To Screen for financial and other sanctions or embargoes.
- For other processing necessary to comply with professional, legal and regulatory obligations that apply to our business, e.g. under health and safety regulations or rules issued by our professional regulator.
- To gather and provide the information required by regulatory bodies or related to audits, enquiries, or investigations.
- To ensure business policies are adhered to, e.g., security and internet use policies.
- For operational reasons, such as improving efficiency, training, and quality control.
- To ensure the confidentiality of commercially sensitive information.
- For statistical analysis to help us manage our business, e.g., our financial performance, customer base, product range or other efficiency measures.
- To prevent unauthorised access and modifications to systems.
- To update and enhance customer records.

- For our legitimate interests or those of a third party, e.g., ensuring we can keep in touch with our customers about existing orders and new products.
- To ensure safe working practices, staff administration and assessments.
- To ensure we are following our internal procedures and working efficiently to deliver the best service to you.
- Marketing our services and those of selected third parties to:
 - existing and former customers.
 - third parties who have previously expressed an interest in our services.
 - third parties with whom we have had no previous dealings.
 - credit reference checks via external credit reference agencies.
 - external audits and quality checks, e.g., for ISO or Investors in People accreditation and the audit of our accounts

The usage information we collect helps us to improve our Platform and to deliver a better and more personalised experience by enabling us to:

- Estimate our audience size and usage patterns.
- Store information about your preferences, allowing us to customise our Platform according to your interests.
- Speed up your searches.
- Recognise you when you use the Platform.

Currently, we do not use the information we gather to show advertising to specific groups our advertisers choose. We will not reveal your personal information for this purpose unless you give us permission. However, if you click on or engage with an advertisement, the advertiser may infer that you fit their target criteria.

Our platform is designed for users who are 16 years old and above. We strictly do not gather personal information of children under 16. If we unintentionally collect such information, we will immediately delete it once verified. If you suspect, we may have obtained personal information from or about a child under 16, please inform us via privacy.inquiries@waterfrontapp.com.

How we get your personal information

We collect information from and about users of the Platform:

- Directly from you when you provide it to us.
- Automatically when you use the Platform.
- From a third party with your consent (e.g., your bank).
- Directly from a third party (e.g., sanctions screening providers, credit reporting agencies, or customer due diligence providers).

As you use our Platform, we may ask for personal information that can identify you, such as your name, address, email, and phone number. Additionally, we may request non-identifying information like your gender, date of birth, and preferred language, including:

- Information that you provide by filling in forms in the Platform.
- Information provided at the time of registering to use the Platform, subscribing to our service, and requesting further or additional services. We may also ask you for information when you report a problem with the Platform.
- Records and copies of your correspondence (including email addresses and phone numbers) if you contact us.
- Your responses to surveys that we might ask you to complete for research purposes.
- Details of transactions you carry out through the Platform and of the fulfilment of your orders. You may be required to provide financial information before subscribing to a service on or through the Platform.

We gather information from different sources, such as our website and communication channels like phone, email, live chat, and social media. This may involve details you give when signing up for our site, subscribing to our services, participating in discussions or competitions, and reporting issues with our site.

We mainly receive your personal information directly from you. Our collection, use, retention, or disclosure of such data is based on lawful grounds. This includes using the information to provide you with a product or service, complying with legal or regulatory obligations, or with your consent.

Automatic Information Collection and Tracking

When you download, access, and use the Platform, it may use technology to collect automatically:

- **Usage Details.** As you use the Platform, we may gather information about your usages, such as traffic, location, logs, and communication data. This includes the resources you access and utilise through the Platform.
- **Device Information.** We may gather data concerning your mobile device and internet connection, such as the device's distinct identifier, IP address, operating system, browser type, mobile network details, and telephone number.

- **Stored Information and Files.** The Platform can retrieve metadata and related information from other files stored on your device, such as photos, audio, and video clips.
- **Location Information.** Our Platform gathers real-time data on mobile device locations in an aggregated format. This data does not contain any personal identification of you or your device. If you prefer not to have this information collected, please refrain from downloading the Platform or remove it from your device.

We do not gather information about your activities over time and across third-party websites, apps, or other online services using these technologies (behavioural tracking).

Information Collection and Tracking Technologies

We may use Web Beacons to collect information automatically. These are small electronic files, also known as clear gifs, pixel tags, and single-pixel gifs, which can be found on pages of our Platform and in our emails. They enable us to track how many users have visited these pages or opened an email. We also use them to record the popularity of certain app content and to check the integrity of our system and servers.

Third-Party Information Collection

When you use the Platform, certain third parties may use automated information collection technologies to collect information about you or your device. These third parties may include:

- Analytics companies.
- Your mobile device manufacturer.
- Your mobile service provider.
- Our service providers hosting the Platform.

Third parties may collect information about you using tracking technologies when you use the platform. They may gather information about your online activities over time, and this data may be linked to your personal information. The information collected may be used to provide you with interest-based advertising or other targeted content. We do not control these third parties or how they use your data. If you have questions about ads or targeted content, please get in touch with the responsible provider directly.

App Stores - External Websites

It's important to note that certain personal information, payment information, and usage-based data may be collected when using an app store like iTunes or Google Play with the Platform. We don't have control over this collection as it's the responsibility of the app store, and their applicable privacy policies will apply. Additionally, the Platform may contain links to third-party websites, but we have no control over their privacy practices or content. It's essential to check the applicable privacy policy and terms of use when visiting other websites.

How long we keep your information

For compliance with regulations and laws, we will keep your personal information only as long as necessary. Afterwards, we will either dispose of it securely or anonymise it. We have a retention schedule to manage the duration of time we keep personal data. If you would like to know the specific timescales listed on it, please get in touch with us using the details provided on this form.

How we protect your information

We understand how crucial it is to keep your information secure. That's why we take extra measures to safeguard your data and prevent unauthorised access, accidental loss, disclosure, or destruction through physical, electronic, and procedural safeguards. However, we cannot guarantee 100% security of your personal information as no data transmission over the internet can be entirely secure. Still, we do our best to protect it from unauthorised access.

To ensure the safety and security of your information, we have implemented measures to secure it from accidental loss and unauthorised access, use, alteration, and disclosure. All the data you provide is stored on our secure servers protected by firewalls.

To ensure the safety of your personal information, we need your cooperation. If we've given you a password to access specific areas of our platform, please keep it private and don't share it with others. We take appropriate measures to safeguard your data but cannot guarantee its security during transmission through the platform. So, please be cautious while sharing any personal information. It's important to note that we are not liable for any security breach resulting from bypassing our privacy settings or security measures.

Where we process your information

We may process information about UK and EU residents outside the UK or European Union. Where this is the case, we will only transfer your information to other countries outside the EEA if it is unavoidable to allow us to deliver our products and services. If we do, we ensure the same level of privacy and security as the UK and EU.

Important Notices to Non-U.S. Residents

The Platform and its servers are operated in the United States. If you are located outside of the United States, please be aware that your Information, including your personal information, may be transferred to, processed, maintained, and used on computers, servers, and systems located outside of your state, province, country, or other governmental jurisdiction where the privacy laws may not be as protective as those in your jurisdiction. If you

are located outside the United States and choose to use the Platform, you irrevocably and unconditionally consent to such transfer, processing, and use in the United States and elsewhere.

How we share your information

From time to time, we may send information to receive information from, or exchange your personal information with:

- Partners or agents who support us to deliver our products and services to you or that we refer you to or refer you to us.
- Companies who perform essential services for us.
- Third-party organisations that conduct research, analysis, and marketing activities on our behalf.
- Regulators, courts, or other public authorities.
- The emergency services in the case of an accident or emergency.
- Law enforcement agencies for the prevention of crime.
- Appropriate authorities to ensure safety, especially considering safeguarding concerns.
- To our subsidiaries and affiliates.
- To contractors, service providers, and other third parties we use to support our business, and those bound by contractual obligations to keep personal information confidential and use it only for the purposes we disclose it to them.
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganisation, dissolution, or other sale or transfer of some or all of Ithaca Clean Energy, Ltd.'s assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by Ithaca Clean Energy, Ltd. about our Platform users is among the assets transferred.
- To fulfil the purpose for which you provide it. For example, if you give us an email address to use the "contact us" feature of our Platform, we will transmit the contents of that email and your email address to the recipients.
- For any other purpose disclosed by us when you provide the information.
- With your consent.
- To comply with any court order, law, or legal process, including responding to any government or regulatory request.
- To enforce our rights arising from any contracts between you and us, including the Platform EULA, Terms of Service, and for billing and collection.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of Ithaca Clean Energy, our customers or others.
- This includes exchanging information for fraud protection and credit risk reduction with other companies and organisations.

We may share information about our users in a way that combines and anonymises it without revealing any specific individual or device.

We may disclose your personal information to a third party for business as described in our Privacy Policy. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

In the preceding twelve (12) months, Company has not disclosed personal information for a business purpose.

We have not sold personal information in the preceding twelve (12) months.

We will only share or exchange data with third parties under the protection of a written agreement and the ability to oversee their activities unless the information is needed for legal or regulatory reasons.

We may receive information about you if you use any other websites or services we operate. In this case, we will have informed you when we collected that data that it may be shared internally and combined with data collected on this site. We are also working closely with third parties (including, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, and search information providers). As a result, we may receive information about you from them.

Our website may have links to and from the websites of our partner networks, advertisers, and affiliates. If you follow a link to any of these websites, please note that they have privacy notices and do not accept any responsibility or liability for these policies. Please check these policies before you send any personal data to these websites.

We may share your information with organisations based outside the UK and European Union. However, where this is the case, we will only do so if the organisation follows local data protection regulations, and it is done under the protection of a written agreement.

If a third party delivers all or part of the service requested by you, whilst the information you provide will be disclosed to them, it will only be used to administer the service provided and maintain management information for business analysis.

Where we have relationships with other organisations that process your information on our behalf, we always ensure they have high data security standards. We will not allow these organisations to use your personal information for unauthorised purposes.

If the business is reorganised or sold, we may transfer any personal information we hold to that organisation.

How you can manage the information we hold and how we use it

We strive to provide you with choices regarding the personal information you provide to us. This section describes mechanisms we provide for you to control certain uses and disclosures of over your data.

- **Tracking Technologies.** You can choose whether to allow the Platform to collect information through other tracking technologies by configuring the applicable settings on your mobile device. If you block other tracking technologies, some parts of the Platform may be inaccessible or not function properly.
- **Location Information.** You can choose whether to allow the Platform to collect and use real-time information about your device's location through the device's privacy settings. If you block location information, some parts of the Platform may become inaccessible or need to be fixed.
- **Promotion by the Company.** If you do not want us to use your email address to promote our services, you can opt out by emailing us at privacy.inquiries@waterfrontapp.com. You can also always opt out by logging into the Platform and adjusting your user preferences in your account profile by checking or unchecking the relevant boxes.

We do not control third parties' collection or use of your information to serve interest-based advertising. However, these third parties may provide ways to refrain from having your information collected or used this way. You can opt out of receiving targeted ads from members of the Network Advertising Initiative ("**NAI**") on the NAI's website.

Data protection regulations mean you have rights in respect of the information we hold about you:

You have the right under the CCPA and certain other privacy and data protection laws, as applicable, to exercise free of charge, your:

- **Right to Know.** You have the right to request information about: (a) the categories of personal information we have collected about you, (b) the categories of sources from which we collected the personal information, (c) the purposes for collecting the personal information, (d) the categories of third parties with whom we have shared your personal information, and (e) the purpose for which we shared your personal information. You may also request information about the specific pieces of personal information we have collected about you.
- **Right to Delete.** You have the right to request that we delete the personal information we collected from you.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- Complete the transaction for which we collected the personal information, provide a service you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
 - Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible.
 - Debug the Platform to identify and repair errors that impair existing intended functionality.
 - Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
 - Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
 - Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the information's deletion may likely render impossible or seriously impair the research's achievement if you previously provided informed consent.
 - Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
 - Comply with a legal obligation.
 - Make other internal and lawful uses of that information that are compatible with the context in which you provided it.
- **Right to Opt-Out.** You have the right to opt out of the sale of your personal information.

In addition, these specific rights are extended to users in the UK and EU:

- **Your right to transparency**
You have the right to know what information is being processed about you and why.
- **Your right to manage consents**

You have the right to consent to us using your data for any activities we do not have another lawful basis to carry out, for example, sending you certain direct marketing communications. You can withdraw consent at any time.

- **Your right to access your data**

You have the right to request access to the information we hold about you; this is called a Data Subject Access Request.

- **Your right to know about sharing**

You have the right to know who your data is shared with and why.

- **Your right to rectification**

You have the right to update your details if they are inaccurate and for information not needed for lawful reasons to be deleted. You also have the right to ask us to complete information you think is incomplete.

- **Your right to be forgotten**

You have the right to ask us to erase your personal information in certain circumstances.

- **Your right to object to processing**

You have the right to object to the processing of your data in certain circumstances. For example, in some circumstances, your information may be transferred to a secondary database in case you want to reactivate your account in the future, and it will be kept and securely destroyed in line with our Data Retention Policy.

- **Your right to restrict processing**

You have the right to have automated processing and profiling restricted. Profiling may be used to analyse or predict economic situations, health, personal preferences, interests, reliability, behaviour, location, or movements. Without it, you may find that the suggestions and guidance you receive from us do not reflect your circumstances very accurately.

- **Your right to data portability**

You have the right to ask us to send information that we process by automated means to you or another nominated data controller in a commonly used electronically readable format.

We will not discriminate against you, in any manner prohibited by applicable law, for exercising these rights.

You do not have to pay any charge for exercising your rights. If you make a request, we will respond to you within one month.

If you wish to action any of the above, please get in touch with us by:

- Emailing ithacacleanenergy@datarepservice.com.
- Writing to Ithaca Clean Energy, C/O Data Rep Service, Friargate Studios, Ford Street, Derby. DE1 1EE.
- Telephoning us at +44 (0)1332 720 078

If you are a resident of the UK and/or EU, you can also complain to the regulatory authority in that country if you are unhappy with how we have used your data.

You can contact them in writing to:

- In the **UK**, the regulator is the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF or call their helpline on 0303 123 1113
- In **Austria**, the regulator is the Österreichischen Datenschutzkommission, Hohenstaufengasse 3 1010 Wien. Autriche
- In **Belgium**, the regulator is the Commission de la protection de la vie privée, Rue de la Presse, 35, 1000 Bruxelles, Belgique.
- In **Bulgaria**, the regulator is the Bulgarian Commission for Personal Data Protection, 2 Prof. Tsvetan Lazarov Blvd, Sofia 1592, Bulgaria.
- In **Croatia**, the regulator is the Croatian Personal Data Protection Agency, Fra Grge Martića 14, HR - 10 000 Zagreb. Croatia.
- In **Cyprus**, the regulator is the Office of the Commissioner for Personal Data Protection, P.O. Box 23378, 1682 Nicosia, Cyprus.
- In the **Czech Republic**, the regulator is the Office for Personal Data Protection, Pplk. Sochora 27, 170 00 Praha 7, Czech Republic.
- In **Denmark**, the regulator is the Datatilsynet, Borgergade 28, 5, 1300 Copenhagen, Danemark.
- In **Estonia**, the regulator is the Estonian Data Protection Inspectorate I, Andmekaitse Inspektsioon, Väike-Ameerika 19, Tallinn 10129, Estonie.
- In **Finland**, the regulator is the Office of the Data Protection Ombudsman, P.O. Box 800, Fin-00521, Helsinki, Finlande
- In **France And French Territories**, the regulator is the Commission Nationale De L'informatique Et des Libertés (CNIL), 3 Place De Fontenoy, TSA 80715, 75334 PARIS. CEDEX 07
- In **Germany**, the regulator is the Virtuelles Datenschutzbüro, C/O Unabhängiges Landeszentrum Für Datenschutz Schleswig-Holstein, Independent Centre for Privacy Protection Schleswig-Holstein, Holstenstraße 98, D-24103 Kiel. Allemagne.

- In **Greece**, the regulator is the Hellenic Data Protection Authority, Kifisias Avenue 1-3, 115 23, Athens, Grece.
- In **Hungary**, the regulator is the National Authority for Data Protection and Freedom of Information, Szilágyi Erzsébet Faszor 22/C, H-1125 Budapest, HUNGARY.
- In **Iceland**, the regulator is the Persónuvernd, Rauðarástíg 10, 105 Reykjavík, Iceland.
- In **Ireland**, the regulator is the Office of The Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois. Ireland.
- In **Italy**, the regulator is the Garante Per La Protezione Dei Dati Personali, Piazza Di Monte Citorio, 121, 00186 Rome, Italie.
- In **Latvia**, the regulator is the Datu Valsts Inspekcija, Data State Inspectorate, Blaumana Street 11/13-11 Riga, LV-1011, Latvia.
- In **Leichtenstien**, the regulator is the Data Protection Commissioner of The Principality of Liechtenstein, Datenschutzstelle (DSS), Kirchstrasse 8, Postfach 684, 9490 Vaduz, Liechtenstein.
- In **Lithuania**, the regulator is the Valstybinė Duomenų Apsaugos Inspekcija, State Data Protection Inspectorate of The Republic of Lithuania, A. Juozapavičiaus G. 6 / Slucko G. 2, 09310 Vilnius, Lithuania.
- In **Luxembourg**, the regulator is the Commission Nationale Pour La Protection des Données 1, Avenue Du Rock'n'Roll, L-4361 Esch-Sur-Alzette, Luxembourg.
- In **Malta**, the regulator is the Office of The Information and Data Protection Commissioner Airways House, Second Floor, High Street, Sliema, SLM 1549, Malta.
- In the **Netherlands**, the regulator is the Dutch Data Protection Authority, Postbus 93374, 2509 AJ Den Haag, Pays-Bas.
- In **Norway**, the regulator is the Datatilsynet, PO. Box 8177 Dep, NO-0034 Oslo, Norvege.
- In **Poland**, the regulator is the Biuro Generalnego Inspektora Ochrony Danych Osobowych (GIODO), Ul. Stawki 2, 00-193 Warsaw, Poland.
- In **Portugal**, the regulator is the Comissão Nacional De Protecção De Dados, Rua De São Bento, 148, 3º, 1200-821 Lisboa, Portugal.
- In **Romania**, the regulator is the National Supervisory Authority for Personal Data Processing, 28-30 G-Ral Gheorghe Magheru Bld., District 1, Post Code 010336, Bucurest, Romania.
- In the **Slovak Republic**, the regulator is the Office For Personal Data The Protection, Úrad Na Ochranu Osobných Údajov, Hraničná 12, 820 07 Bratislava 27, Slovak Republic.
- In **Slovenia**, the regulator is the Information Commissioner, Namestnik Varuha Clovekovih Pravic, Vošnjakova 1 P.P, 78 1000 Ljubljana, Slovenia.
- In **Spain**, the regulator is the Agencia De Protección De Datos, C/ Jorge Juan, 6, 28001, Madrid, Espagne.
- In **Sweden**, the regulator is the Datainspektionen, Drottninggatan 29, 5th Floor, Stockholm, Suede.

Cookies

Our website uses cookies to differentiate you from other users. This enables us to enhance your browsing experience and optimize our website's performance. For more information on our cookies and their purpose, please refer to our Cookie Policy available on our website at www.ithacacleanenergy.com.

Changes to this policy

Our policy undergoes regular reviews, and any future changes will be posted on www.ithacacleanenergy.com. This way, you can access the latest version at any time.

This Privacy Notice is the 6th June 2023 version (ITH0023 v1.2 06.06.23).

Document Version History

Date	Author	Version	Notes
May 19, 2023	Khalid Kamhawi CEO	1.0	Draft notice created.
June 06, 2023	Kieran Morgan-McGeehan (Data Rep Service) Director, Business, Risk & Compliance Consultant	1.2	Notice revised and adopted.