I-REC Services BV/Evident Privacy Notice

Your data security and privacy are important to us. Evident ensures integrity and confidentiality in the process of collecting and storing personal data. We will only use and collect personal information that is necessary for our business operations, and it will be handled and used in accordance with our Privacy Policy.

This privacy policy covers the processing of your data while using this website as well as a guide to how we process data in the course of a commercial relationship with Evident. This Privacy policy complies with the EU GDPR, UK GDPR and Data Protection Act, and global data protection legislation and best practices.

Our Contact Details

Registered Office:

Achter de Tobrug 151, 5211SM, 's-Hertogenbosch, The Netherlands**.**

Head Office/Operations Centre:

1a Southbourne Road, Sheffield, South Yorkshire, S10 2AE, United Kingdom.

General Enquiries: helpdesk@evident.services

Privacy/Data processing enquires: dataprotection@pure-energi.com

Definitions:

Personal information: Data that can identify an individual and can include but is not limited to: a person's name, address, email address, phone number. Personal data does not include encoded and anonymised data.

We/Our/Us: refers to I-REC Services B.V. also known as Evident.

Site User: refers to the website user but who is not necessarily in a commercial relationship with us.

You/Your/Data Subject: refers to a site user, an individual in a commercial relationship with us or an employee or agent of a company/business in a commercial relationship with us. Please note, a data subject can fit more than one of these criteria.

The Site: refers to our websites.

Subject Access Request: a request made by you to our DPO about what data we have on you as well as to request the status of our processing of your data.

EU GDPR: European Union General Data Protection Regulations.

UK GDPR: United Kingdom General Data Protection Regulations (different from Data Protection Act 1998 which supplements the UK GDPR)

DPO: Data Protection Officer

Principles

We process your data in accordance with the principles of:

- Fairness, lawfulness and transparency.

- Collection of data for specific, explicit and legitimate purposes.
- Adequacy, relevance and limitation of data to what is necessary.
- Accuracy of data and facilitating rectification of inaccurate data.
- Reasonable retention of data for no longer than is necessary.
- Security of data
- Safeguarding data during transfers.

Legal basis for data collection and processing.

As a site user, the legal basis for collecting and processing data about the use of the website is our legitimate interest. As an individual in a commercial relationship with us, the legal basis for collection and processing of your data is part of our contractual obligation. For employees or agents of a company in a commercial relationship with us, we rely on our legitimate interest arising from the contract between your employer and us as the legal basis for the collection and processing of your personal data. For individuals who have been in communication with us beyond the website but are not yet in a commercial relationship with us, the legal basis for processing your data is our legitimate interests and your consent if you contact was initiated by you.

Information we collect, how we collect it and how it is used.

We collect information with regards to how the Site User uses the Site, this is usually anonymous and helps to provide information as to the ease of use, accessibility and performance of the website. We also collect information from individuals at the start of a commercial relationship, this may include name, address, email, phone number, national identification documents and work information. This information is required at the start of a commercial relationship to facilitate the provision of our services to you. This information is usually collected through the appropriate application forms on the Issuer or Code Manager's website.

When you send communications to us, we may retain and use these communications in order to process your enquiries, respond to your requests, and improve our services.

We will share this information with other organisations, if necessary for the provision of our service to you or in facilitating the exercise of your right to portability, where that applies. Please see the Business Transfers section of this policy for more information.

It is our policy not to use or disclose confidential or non-public information received from clients except in connection with the provision and improvement of our services. Such uses or disclosures may include, for example, those that are usual, appropriate, or acceptable to carry out the service for which the information was given.

We do not disclose confidential or non-public information to third parties for their direct marketing purposes nor do we endorse or promote offers from third party advertisers.

We may from time to time, in accordance with this Privacy Policy, use personal, confidential, or non-public data to inform a client or customer about products and services that we expect may be of interest to them. Individuals may object to any such data being used for such marketing purposes by contacting us in writing at the address or email below.

External websites

Our website occasionally links to other websites for additional information. The Company does not

control and is not responsible for how these external web sites collect and use information. This privacy statement applies only to our own domain, evident.services and evident.app

Your right to opt out:

As a site user, you can opt out of data collection and usage. Please see our cookie policy for more information on how to opt out of data collection. You can also contact the DPO to request restricted processing or erasure of your data.

As an individual in a commercial relationship with us, consent to collecting and processing data is drawn from the contractual agreement. To end the processing of data, you may contact the DPO to request a restriction of processing, such that no other communication is made with you other than for the purpose of ensuring termination of the contract. Upon termination of the contract, data will be retained in line with the retention policy set out in this policy and will only be stored in line with our obligations under the retention policy.

As an employee or agent of a company or business in a commercial relationship with us, you have a right to restrict processing of your information by contacting the DPO. Reasonable steps will be taken alongside your principal or employer to ensure that a replacement contact at the company is made available, after which your data will be fully and permanently deleted.

Third Party Processors

We process all the data we collect through Pure Energi Limited who adhere to data protection legislation in the UK, EU and globally. Additional safeguards are put in place by Pure Energi to ensure that data is kept securely, processed in line with this policy and protected where international transfers take place.

Pure Energi Limited stores and processes information using infrastructure of cloud service providers. Pure Energi Limited has ensured that it uses a cloud service provider whose compliance with data protection legislation is robust enough to meet its requirements. Safeguards such as encryption are also in place to ensure that data is secure. Pure Energi Limited's cloud service providers also ensure that only authorised personnel have access to servers where data is stored and processed.

Data storage and retention:

Your information is securely stored in the United Kingdom.

For individuals in a commercial relationship with us, data that is provided to us at the start of the commercial relationship will be kept throughout the course of the relationship with us. For employees of companies in a commercial relationship with us, data is kept throughout the course of your principal's relationship with us or until you request restriction or objection to processing of your data.

Data on the Registry is never deleted. This is needed for our audit trail purposes. These audit purposes are for our legitimate interests and fall under the scope of lawful basis for processing relating to archiving data for historical research purposes. Such data will include, usernames, names, telephone number and emails that have been provided in the course of your commercial relationship with us. We will employ further safeguards of restricted processing, pseudonymisation, and invisibility of such data. **You retain the right to access or request what information we have on you in the registry**. However, once a commercial relationship has ended, the right to rectification no longer applies as the data is historical.

Only data on the Registry is kept in this manner, where the data is kept elsewhere, we keep your data for we keep your data for eighteen months, except contracts which we will maintain a copy of for our business records. We keep data for this period for dispute resolution purposes, national legislation complaince purposes and outstanding billing purposes. After this time period, data is deleted.

We take reasonable precautions to protect personal, confidential, and non-public information. It is our policy to restrict access to confidential, non-public, and personal information to those employees who need to know such information in order to provide our services or as otherwise appropriate and consistent with this Privacy Policy.

Your rights

- You have a **right to be informed** of the data we collect, when we collect it, how we use it and changes to the way we process your data.
- You have a **right of access** to the data we hold on you by submitting a subject access request to the DPO through the stipulated means in the next section of this policy.
- You also have a **right to rectify** data that is held by us, where there is reason to believe that such data is inaccurate.
- You have a **right to the erasure** of your data (in line with our retention policy). You have a right to restrict processing of your data.
- You have a **right to object to automated decision-making** including profiling.
- Site users and employees or agents of companies in a commercial relationship with us have an additional **right to object** to our processing of your data, please see the information above on data storage and retention. You do not have a right to data portability as our processing of your data is only for our legitimate interests.
- While the right to object does not apply to individuals in a commercial relationship with us, the **right to withdraw consent and restrict processing** in line with the right to opt out will apply.
- Individuals in a commercial relationship with us also have a **right to portability** in order to securely move and use your data across a range of services without having to provide such data again, also see the business transfers section for more information.
- Individuals who have been in communication with us beyond the website but are not yet in a commercial relationship with us have the same rights as employees of client companies.

The ways in which these rights can be exercised and clearly stated throughout this policy document, and you can contact the DPO for more information or to make a request to exercise these rights.

Additionally, employees or agents of companies in a commercial relationship with us must bear in mind, that we act as a joint controller with their principal who provided their details to us, for the purposes of fulfilling our contractual obligation, hence, the employer or principal, themselves must be contacted by you for processing of your data that does not relate to the commercial relationship, we have with them.

Subject Access Request

EU data subjects: Email or write to the DPO or the EU Representative.

Data subjects in non-EU countries: Email or write to the DPO.

It is recommended that a copy of ID is attached to your letter or email, as we cannot process a request unless we are able to identify the individual. More information may be requested for the purpose of identifying the individual to prevent unauthorised access.

More information may also be requested with regards to the Subject Access Request itself to ensure that the request is dealt with effectively.

While, legally, we have a month to respond to requests, we aim to acknowledge receipt of subject access requests and request additional information, if necessary, within seven business days of receiving the request. Upon the receipt of all necessary information and proper identification of the data subject, we aim to process and complete the request within a further 14 business days.

Where there is an urgent reason for faster processing of a subject access request, the data subject must state that it is urgent and the reason for such urgency. It is recommended that urgent subject access requests be by email.

Requests will be responded to in the same manner as it has been received unless the data subject requests otherwise in the initial or subsequent communication.

DPO

Name: Michelle Aipime

Correspondence Address: Pure Energi Limited, 1a Southbourne Road, Sheffield, S10 2AE, South Yorkshire, United Kingdom.

Email: dataprotection@pure-energi.com

The DPO is also the UK representative for Evident data subjects based in the United Kingdom.

EU representative

Under the EU GDPR, we hereby provide the EU representative below as an additional contact point for data subjects based in the EU. Please note the EU representative can only deal with requests relating to data subjects in the EU.

Name: Jared Braslawsky

Correspondence Address: Achter de Tobrug 151, 5211SM, 's-Hertogenbosch, The Netherlands

Email: eudata@pure-energi.com

Information Disclosure Obligations under national laws

Personal data held by us will be treated with the utmost confidentiality. However, where we reasonably suspect criminal activity, we will disclose such information to the appropriate authroities. Likewise, where we are bound by national laws to make certain disclosures to public authroities or regulatory bodies or bound by court order to make such disclosures in a legal proceeding, we will comply with such obligations.

We will only inform the data subject of such a disclosure if the law or court order in question permits it.

Public Data published by other sources:

This policy does not apply to data that is publicly available. However, where such data has been deleted/erased from the source upon the request of the data subject or to comply with a court order, law or other code of conducts/guidelines, we will also erase any duplicates of such data on our systems at the request of the data subject.

Public Data Published by us:

Data may be made public by us, this may include client energy device information (which stays on forever, but upon termination of our contractual relationship, it will be made clear that I-RECs are no longer being issued against the device), list of participants and registrants (information here will be removed upon contract termination). Such data is only made public according to the Standard terms agreed upon between you and us upon the commencement or continuation of a commercial relationship and in fulfilling our obligations in line with regulations. Where our commercial relationship comes to an end, and such data is no longer public, and we will take reasonable and practical steps to ensure that processors or joint controllers whom we have shared such data with and other parties who access this data from us also erase their copies of the data. However, we cannot guarantee that such data will be made completely private due to the nature of the internet, especially as the basis of making the data public was based on the terms of our contract.

Data security and protection

We ensure that data is kept secure using industry standards on information security management. However, there is no guarantee that measures for security will always prevent unauthorised access. Where unauthorised access occurs, we will notify you, take reasonable steps to remedy the situation and to mitigate it in the future.

Where we communicate through electronic means with you, we will also ensure that we take all reasonable steps to ensure that our medium is free from viruses and is secure. However, we cannot guarantee absolute security as no method of transmission over the internet is 100% secure. Consequently, we cannot ensure or warrant the security of any information you transmit to us, and you do so at your own risk.

We also urge you to take reasonable steps to ensure that there is no unauthorised access to your data by ensuring that your devices and credentials are kept safe and private.

Breach

In the event of a data breach, the Information Commissioner's Office (ICO) and/or Dutch Data Protection Authority and the affected data subjects involved will be notified. Where it is not possible to give individual notice to you, a public notice will be placed on this website.

Business transfers

Apart from processing with the aforementioned processors, we also share data with the Central Issuers, your country's Issuer, Registry operators, Platform operators and the International REC Foundation. This will be in order to comply with the Foundation's International Attribute Tracking Standard, the Evident Product Code, appropriate contractual obligations and national legislation.

We may also get information from the Businesses we have commercial relationships with in the course of providing services to you and them. The information we get is your name, contact details, activities carried out between parties under contract relating to the issuance or redemption of I-RECs. We get this information from the Central Issuers, your country's Issuer, Registry operators, Platform operators.

When making such data transfers, we will ensure the security of that data by using means which are encrypted and free from viruses. We will also ensure that only data that is necessary for the transfer or processing by the recipient is transferred to comply with the data minimisation principle. Where any records of your data have been erased in compliance with this policy, we will alert any recipients of such data to delete their copy of the data.

More information on the relationships between different Accredited Entities and Market Entities and reasons for sharing data between them, are made available in the Product Code or International Attribute Tracking Standard. Data is only shared in this manner to comply with our obligations, provide our services to you or other related entities and for our legitimate interest. Data will never be shared for the purposes of direct marketing.

For MiQ users

We share your data frequently with MiQ Services for the purposes of delivering their product on our Registry and in compliance with the MiQ Program Guide and MiQ Standard. We have an EU GDPR and UK GDPR compliant Data Sharing Agreement with MiQ Services. Our processing of your data on the Registry will continue to be in line with this Privacy Notice, however, MiQ Services is also a joint controller of your data on the Registry.

Changes to this policy

If in the future, changes are made to this Privacy Policy, we will post the new policy on this website. If the new policy is somehow materially less restrictive or protective of your privacy than the current policy, we will not apply the less protective aspects of the revised policy to information you have previously provided to us without first obtaining your consent.

We reserve the right to change this Privacy Policy in the future. Your continued use of this website and our services following a change in the Privacy Policy represents consent to the new policy to the fullest extent permitted by law.

We will not process your data in any way that violates your contractual agreement with us.

We encourage you to periodically review this Privacy Policy.

This Privacy Statement was last updated on 09 July 2021.

Questions

For questions regarding this policy or your data and how we process it. Please contact the DPO listed above.

Further details on the acceptable use of our services can be found in our Standard Terms and Conditions for the respective services we provide to you.

How to complain.

You can contact the DPO directly to complain at dataprotection@pure-energi.com. You can also complain to the Dutch Data Protection Authority if you are unhappy with how we have used your data or managed your complaints about your data. You can contact them by writing to them: Autoriteit Persoonsgegevens, PO Box 93374, 2509 AJ DEN HAAG or by telephone +31(0)708888500.

You also have a right to complain to your local data protection authority where appropriate.