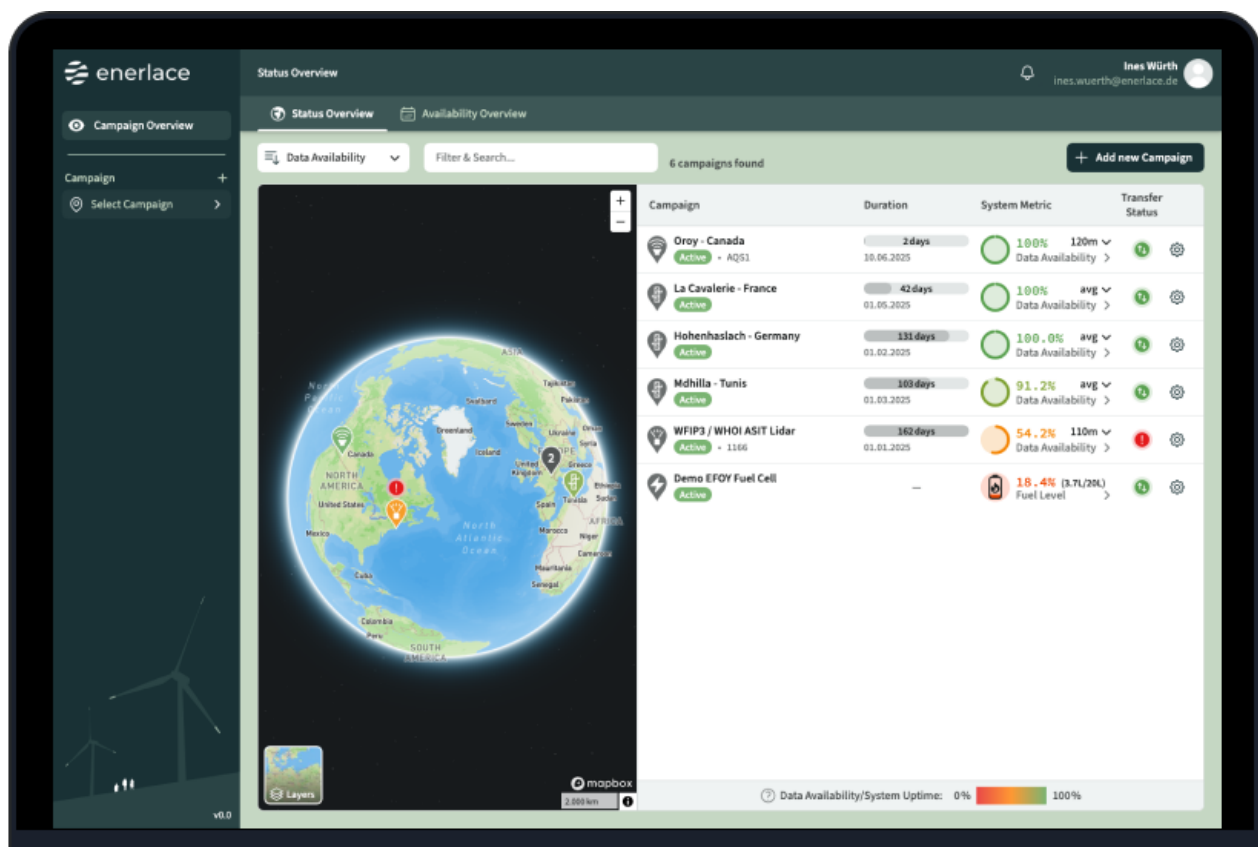


Cybersecurity in Enerlace's *Moli* wind monitoring software

Document classification	Public
Document reference	WP 2025-02 Version 1
Lead author	Andrew Clifton
Checked by	Ines Würth
Last revised	21 November 2025
Contact	Email: andy.clifton@enerlace.de Tel: +49 1745 60 20 90

Released by Enerlace GmbH, Badgasse 13, 72280 Dornstetten, Germany.

Find out more about us at www.enerlace.de.



Cybersecurity in Enerlace's *Moli* wind monitoring software

Enerlace White Paper WP2025-02 Version 1 (21 November 2025)

Moli is Enerlace's wind data monitoring platform designed for high reliability, transparency, and security. This white paper outlines how *Moli* protects data confidentiality, integrity, and availability whether *Moli* is hosted on our own infrastructure or deployed on client servers.

We welcome all feedback and would appreciate your perspectives on this important topic. Please do not hesitate to get in touch with us with any comments or questions.

Thank you for working with us!



Ines Würth, Dr.-Ing.
Managing Director, Enerlace GmbH



Andrew Clifton, Dr sc.
Managing Director, Enerlace GmbH

Table of Contents

1	Introduction and executive summary	1
2	What is wind data monitoring, and what is <i>Moli</i> ?	1
3	<i>Moli</i> 's servers	2
4	Getting started with <i>Moli</i>	2
5	Data transfer to <i>Moli</i>	3
6	Knowledge Base	4
7	Activity logs	4
8	White labeling.....	4
9	Self-hosted deployment	5
10	Data protection and privacy	5
11	Software updates and patches	6
12	Incident response.....	6
13	Conclusion: secure data monitoring with <i>Moli</i>	6
14	Frequently asked questions.....	6

1 Introduction and executive summary

Moli is Enerlace's secure, web-based platform for automated wind data monitoring, designed to streamline workflows and help ensure high-integrity measurement campaigns. It supports flexible deployment – either on Enerlace-managed, ISO 27001–certified EU servers or on client infrastructure – while offering robust authentication, role-based access control, and full organisational transparency.

Moli employs modern application security, encrypted data handling, GDPR-compliant privacy measures, and continuously monitored infrastructure. With strong incident response processes and alignment to international standards, *Moli* delivers reliable, protected, and traceable wind measurement data, enabling customers to manage campaigns efficiently and confidently.

2 What is wind data monitoring, and what is *Moli*?

Wind data monitoring is the process of regularly, rapidly, and reliably checking wind measurements from ongoing measurement campaigns to check that the measurements are being recorded, quantify data availability, do basic quality checks on the data, and make sure that campaigns are proceeding as planned.

Moli is Enerlace's web-based wind monitoring and data management software. It automates much of the process of checking data from wind measurement campaigns so that experts are freed up from repetitive, time-consuming work and have more time available to focus on applying their skills.

Moli is designed to ingest data from your met masts, wind lidar, sodar, and fuel cells into a data lake and then display it (Figure 1). Data are checked automatically and alarms are sent to users by email for certain events or conditions. Data can also be presented in a PDF report.

Moli is continuously updated using feedback from customers and following our own roadmap.



Figure 1 *Moli* ingests data from a users' wind measurements. Data are processed, checked, and displayed for multiple users through their browser. Photo credits: Lidar trailer image © GWU Umwelttechnik 2023. Sodar image © AQ System AB 2025. Power system image © EFOY 2025. Met mast image © Andrew Clifton 2010. All images used with permission.

The information in this white paper is focussed on data security and personal data protection. We would be happy to provide a short demonstration of Moli for context. Please contact andy.clifton@enerlace.de to arrange a demonstration.

3 Moli's servers

Moli is hosted on servers operated by Hetzner Online, located in Nuremberg and Falkenstein in Germany.

Hetzner is certified to ISO 27001:2022, the world's best-known standard for information security management systems (ISMS). For details of the certification including awarding body, see <https://www.hetzner.com/unternehmen/zertifizierung/>.

4 Getting started with Moli

4.1 Registering as the first user for a company

We provide a self-service registration for Moli. Users can register at <https://moli.enerlace.de/register>. During the registration process users are asked to provide some information including name, email address, and organisation name, e.g. *Eastern Wind Company* or *Southern Service Provider*.

Users then go through an email verification process before their account is created.

The first person to register using a particular organisation name becomes an administrative (admin) user for the organisation they created.

We track the creation of new organisations in Moli to look out for duplicate organisations being set up by users from the same company. We have processes in place to consolidate these organisations.

4.2 Adding users to Moli

Admin users can send invitations to their colleagues to join them on Moli. This is done from within Moli and is done by sending an invitation.

They must choose a user type – admin (highest rights), member, or guest (lowest rights) – when they send the invitation. Each new user must confirm their email address, create an account with their email address and a secure password and accept a user agreement to access Moli.

Users are then added individually to each campaign as either a guest or a member. They may be given lower rights but not higher ones in the campaign compared to their status in the organisation. That means an organisation member can be a guest in a campaign, but an organisation guest, can only be a campaign guest and not a member.

The following personal data are stored in Moli for each user:

- Email address (confirmed via users clicking on an email they receive)
- First and last names (not verified)
- Organisation they were invited to.

We do not check if the persons being invited have permission to see the data in Moli. It is possible for Admin users to check who has access to Moli, and we recommend that companies review this information regularly.

A user in Moli can belong to multiple organisations.

4.3 User authentication and logging in

Login to Moli is through a username and password. Minimum complexity requirements apply.

Users may enable two-factor authentication within Moli.

4.4 Joining an existing organisation

Persons wanting to use Moli should ask their admin user to send them an invitation to use Moli.

Users can also contact Enerlace at support@enerlace.de to find out if their organisation is already using Moli. We will check with the admin user before providing any information.

4.5 User management

Moli's role-based access control defines three main levels of access:

- Admin: Full control over all aspects of Moli, including actions that might incur costs.
- Member: Can view and manage projects and campaigns but not change organisational settings.
- Guest: Read-only access to assigned data or dashboards.

Admin users can see all other users in their organization and immediately downgrade or remove access.

5 Data transfer to Moli

Data can be transferred to Moli via the internet and into the app by drag-and-drop uploads, SFTP, or email (Table 1).

Table 1 Data can be securely uploaded to Moli in the app, via SFTP, or via email

Transfer method	Description	Security measures
Via drag-and-drop in the app	In-browser data transfer into a campaign	• Data can only be uploaded by logged-in users with sufficient rights
Via SFTP	Files can be uploaded to Moli via SSH File Transfer Protocol. This can occur by: 1. directly from the measurement device	• Each campaign has a discrete storage space that is protected with a username and password.

	- from the measurement device vendor's own servers, e.g. Vaisala's <i>Windcube Insights</i> portal - by a transfer from another SFTP server or using an SFTP client	- The username and password are only available to logged-in users with sufficient rights - SSH-Key-based server access
Via email	Files can be sent to Moli via email. This may occur via: - Data sent by the measurement device - Data sent by the vendor's own servers - Data sent by a third-party contractor - Data sent by the device owner, e.g., by forwarding data received via any of the other options.	- Each campaign has a discrete email address - The reception is via secure SMTP connections (TLS)

All data files successfully uploaded to Moli must pass data checks. These checks are primarily to avoid data being associated with the wrong campaigns. We look for things like:

- Correct file extensions
- Correct file format
- Presence of the correct serial number or other metadata in the file headers.

6 Knowledge Base

We maintain a knowledge base at <https://enerlace.notion.site>. This contains a wide range of articles related to Moli.

7 Activity logs

We generate extensive logs for Moli, including information about data uploads, issues, and system actions. Some of this information is available through Moli's own campaign-level logbook. More detailed information may be available upon request.

8 White labeling

Moli can also be white labelled. Options include:

- Custom URL (may require support from an IT team to add DNS entries)
- Custom log-in page
- Registration process branded following corporate requirements
- Custom terms and conditions.
- Custom colors and logo, including on the report.

Please contact andy.clifton@enerlace.de for more information.

9 Self-hosted deployment

As well as our hosted *Moli* option, we also offer the option to deploy *Moli* as self-hosted software, running on your own infrastructure. We install *Moli* for you, and you retain full control over infrastructure access and network configuration. Depending on your requirements, we may also develop new features or workflows for you as part of the deployment.

We call this our „Enterprise“-level option. This option is subject to additional fees depending on the scope of the deployment.

Please contact andy.clifton@enerlace.de for details.

10 Data protection and privacy

Data security and privacy are integral to *Moli*'s design. All sensitive data is handled according to EU and industry best practices:

- Backups are encrypted and retained according to EU data protection standards.
- Access to sensitive data (e.g., API keys, credentials) is restricted and logged.

We aim to comply with regional data protection requirements, including:

1. **European Union (GDPR).** We comply with the General Data Protection Regulation (GDPR). Users in the EU have rights including access, rectification, erasure, restriction of processing, data portability, and objection.
2. **United Kingdom (UK GDPR).** We comply with the UK Data Protection Act 2018 and UK GDPR. Users in the UK have the same rights as those in the EU, including access, rectification, erasure, and data portability. Enerlace GmbH is registered with the UK Information Commissioner's Office, registration number ZB933546.
3. **Canada (PIPEDA).** We comply with the Personal Information Protection and Electronic Documents Act (PIPEDA). Users in Canada have rights including consent, access, and rectification of personal information.
4. **United States (California – CCPA).** We comply with the California Consumer Privacy Act (CCPA). Users in California have rights including access, deletion, and the right not to be discriminated against for exercising these rights.
5. **Australia (Privacy Act 1988).** We comply with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). Users in Australia have rights including access to and correction of their personal information. If data is stored outside Australia (e.g., in the EU), we ensure it is protected under safeguards comparable to those required by the APPs. In case of a breach likely to cause serious harm, we will notify affected users and the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches scheme.

For more information or to exercise your rights under these regulations, please contact our data protection officer at support@enerlace.de.

11 Software updates and patches

Moli is updated according to an internal feature roadmap which is informed by feedback from our users. Updates may also include security features. Details of these updates are captured in release notes which are available in the Moli Knowledge Base.

Regular system monitoring and rapid patching ensure that Moli remains secure and resilient.

12 Incident response

We have documented processes for reporting and handling security incidents.

Please report any security incidents to us at support@enerlace.de. If you are concerned that email security may be compromised you may reach Andrew Clifton at +49 1745 60 20 90.

13 Conclusion: secure data monitoring with Moli

Moli's cybersecurity model provides flexibility without compromising safety. Whether hosted by us or deployed in your own environment, Moli's layered security approach ensures that sensitive wind measurement data remains protected, traceable, and accessible only to authorised users.

14 Frequently asked questions

	Question	Answer
0	Does Moli comply with GDPR requirements?	Yes. Moli processes personal data in accordance with the GDPR. Data processing takes place exclusively within the EU.
1	Where is the data centre located?	The Moli application is hosted on servers provided by Hetzner. The data centres are in Nuremberg and Falkenstein, Germany.
2	What are the interfaces to Moli?	Moli offers several secure interfaces for data transfer and system integration: • SFTP upload: Campaign-specific SFTP access for automated data transfer. Credentials (username, SSH key) are unique per campaign. • Email import: Alternatively, files can be sent via email to a campaign-specific address. Emails are received over secure SMTP (TLS). • Web upload: Manual upload of files via the HTTPS-secured Moli web interface. • API (internal): REST-based interfaces for internal communication and process control. All interfaces use encrypted connections (TLS/SSH) and are isolated per campaign to prevent unauthorised access.
3	Is there an availability monitoring system?	Yes. System availability is monitored using Datadog (server, service, and performance monitoring) and Sentry (application error and exception

		tracking). These tools enable continuous monitoring and early detection of issues.
4	How does the user rights and permissions concept work?	The user model includes: • User accounts with role-based access control (e.g., Admin, Member, Guest). • Authentication via password with active password policies. • Optional two-factor authentication (when available). • No access without invitation by campaign admins.
5	Who can create users and assign passwords?	New users can only be created by organisation admins within Moli. Passwords are set by users themselves through the invitation and reset process (no passwords are ever transmitted or stored in plain text).
6	How long are personal data retained?	Personal data (e.g., user accounts, log entries) are stored only as long as necessary for operation. When a user is deleted, associated personal data are deleted as well.
7	Who is responsible for editing/deleting permissions, and how is this managed?	Organisation admins manage permissions through Moli's user management interface.
8	What is logged?	The following are logged: • User logins and failed attempts • File imports and deletions • Changes to campaign configurations • System events (e.g., reprocessing, job errors) • IP addresses of accesses (deleted after a defined retention period)
9	Is there access to log files? If so, who has access?	Only system administrators (DevOps / backend team) have access to system logs. Users do not have access but can view campaign-related events via the campaign logbook.
10	Is there a backup concept?	Yes. Regular backups of databases and user data are performed. Backups are encrypted, tested regularly, and stored at two independent locations.
11	Are recovery tests performed?	Yes, backups are regularly tested for recoverability.
12	Is there a disaster recovery plan for Moli?	Yes, a disaster recovery plan exists.
13	Are there patch management processes?	Yes. Security and system updates are applied regularly (automatically or manually by DevOps). Critical security updates are implemented immediately after release.
14	Are there incident / problem / change management processes?	Yes. Incidents are recorded via email at support@enerlace.de and prioritised based on severity. Problems and change requests can be submitted through the same channel at any time.
15	Vulnerability management?	Yes, regular security assessments are conducted.
16	Are there SaaS system hardening measures?	Yes. Minimal attack surface ensured through:

		• Access only via HTTPS • Firewall rules • SSH key-based server access • No unnecessary open ports • Use of proven languages, frameworks, and components • Optional 2FA (when enabled by users)
17	When are temporary files deleted?	Non-personal data and files are deleted after their corresponding entities are removed from the system, with a delay also applied to backups.
18	How is data encrypted?	In transit: TLS 1.2+ At rest: Passwords are stored using salted hashes (e.g., <i>bcrypt</i>).
19	Is there antivirus protection for the cloud application?	Since the setup is based on Linux (not vulnerable to typical viruses), no antivirus software is used. The system is regularly checked for vulnerabilities using <i>chkrootkit</i> .
20	Is there a vulnerability reporting process?	Yes. Discovered vulnerabilities are recorded internally, prioritised, and tracked with version history.
21	Is there a security incident reporting process?	Yes. Security incidents are documented, evaluated, and concluded with a post-mortem process. If personal data are affected, GDPR-compliant notifications are issued to affected parties.
22	Does Enerlace provide its own data processing agreement (DPA)?	No.

Contact

If you have any questions, comments, or would like to discuss this in more detail, please contact:

Andrew Clifton (Managing Director)

Tel: +49 1745 60 20 90

Email: andy.clifton@enerlace.de



About Enerlace

Who We Are

Enerlace was founded by Dr.-Ing. Ines Würth and Dr. sc. Andrew Clifton, who together bring 35 years of experience in making meteorological measurements for wind and solar energy, and environmental science.

Frustrated by how much manual work is required to manage data - and how rarely it is FAIR (findable, accessible, interoperable, reusable) - they created Enerlace to bring digitalisation and automation to renewable energy.



Dr.-Ing. Ines Würth



Dr. sc. Andrew Clifton

Ines and Andy are both Managing Directors of Enerlace GmbH.

Ines is Enerlace's product owner and an internationally recognised expert in the use of wind lidar. She trained as an aerospace engineer at the University of Stuttgart before joining the Chair of Wind Energy as a researcher. Ines later became the leader of the Testing & Measurement Group. Ines gained her PhD in minute-scale forecasting of wind power using long-range lidar data in 2021.

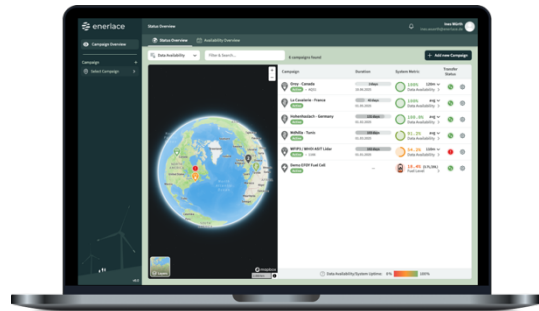
Andy leads Enerlace's sales and is the first point of contact for new customers. A pioneer in the use of wind lidar for wind energy, he deployed his first wind lidar in 2008. Andy wrote the IEA Wind Recommended Practices for Wind Lidar in 2013, led IEA Wind Task 32 on wind lidar from 2018 to 2022, and now leads the digitalisation working group in IEA Wind Task 52, "large-scale deployment of wind lidar".

Ines and Andy are supported by a team of experienced software developers.

What We Do

Our mission is to accelerate wind energy deployment by automating repetitive and complex tasks, freeing experts for high-value work.

This mission drives Moli, our software for monitoring and managing wind measurement data.



Our Story

Enerlace began in 2023 as a spin-off from the University of Stuttgart and became an independent company in 2024, focused on software for renewable energy and climate-related data.

Customers on 3 continents now use Moli for projects in over 20 countries worldwide.

Where We Are

We're based in Dornstetten, a medieval town in Germany's Black Forest.



Find out more

See our website at www.enerlace.de or contact us at info@enerlace.de.

Document ends here