FACTSHEET **SAFETY**

Seven measures ensuring the security of Data Safe House

To realise the energy transition, grid operators need insight into the future plans of the industry. However, these sustainability plans are confidential. In Data Safe House, these plans are stored securely and shared with authorised parties. To maintain the confidentiality of this information, we employ a number of stringent security measures.

1 CISO

Data Safe House employs a Chief Information Security Officer (CISO), Wil van Egdom, who brings extensive experience to the role. He has performed a thorough risk analysis to identify unique risks specific to Data Safe House, leading to the implementation of targeted security measures.

In his capacity as CISO, he continuously oversees the security of our data and processes.

2 Best practice to stay secure: ISO 27001

Data Safe House is ISO 27001 certified across the entire chain. That is: our cloud provider, the IT platform and the organisation itself. Employees are made aware of information security in training courses.

With ISO 27001 as a recognised standard for information security, we ensure ongoing security by adhering to the *Plan, Do, Check, Act* cycle. Security measures are planned (*Plan*) and implemented (*Do*). Regular checks are conducted (*Check*) to ensure adequacy, and adjustments are made as necessary (*Act*). This cycle ensures continuous improvement and adaptation to new risks.

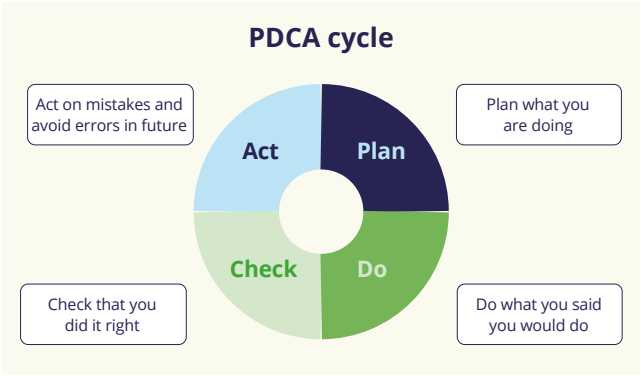
3 Audit by an independent party

Both our technology and our administrative processes undergo regular audits by independent parties to verify compliance with ISO 27001 standards.
We also conduct regular penetration tests on our IT platform to identify and mitigate potential vulnerabilities.

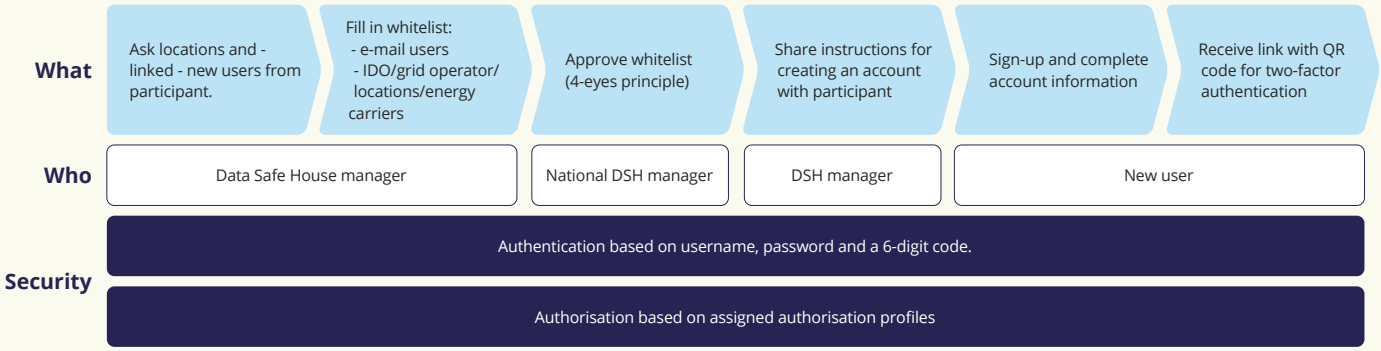
4 Data server security

The Data Safe House solution utilises a *three-tier* architecture, separating the web server (1), database (2), and application server (3). This separation ensures that a hacker cannot access participant data or sustainability plans through the website.

Even if access to the database is gained, data remains inaccessible due to encryption. All communications between servers are encrypted, both over the public internet and within the data centre. All comprehensive measures are in place to prevent eavesdropping.



A secure login process step by step



5 Identification and access control

Access is granted on a personal level using two-factor authentication.

6 Authorisation profiles on need-to-know basis

Data Safe House operates with authorisation profiles that define data access on a need-to-know basis.

Companies can access only their own data, while the Data Safe House manager is the only person who can view all data within his own industry cluster. Other Data Safe House employees do not have access to the data. Data requesters, such as grid operators, only access data relevant to their operational cluster and energy carrier.

Access does not imply usage. To utilise data for specific analyses or studies, parties must submit a data request. Within the Data Board, the participants discuss the data request. If the applicant is allowed to use the data, this will be for a specific period for the specific purpose of the application.

Authorisation is based on the **need-to-know** principle, only access to what is needed.

Appropriate authorisation profiles are **managed** by the **Data Safe House manager**.

Assigned authorisation profiles are **periodically reviewed** and adjusted as necessary

Each **individual** (email) is assigned an authorisation profile with a **recorded term**.

7 Scheme

In addition to technical measures ensuring confidentiality, Data Safe House has established Terms of Use. By signing these, participating parties commit (among other agreements) to treating data confidentially and using it solely for the agreed purposes. Only industry parties, grid operators, and network parties who sign these terms are permitted to participate in Data Safe House.

Trust: key to a successful energy transition

Trust of industry parties in Data Safe House as a secure environment to share sustainability plans, and confidence in the accuracy and completeness of the data from grid operators, are crucial for the success of the energy transition. The seven measures outlined above ensure the highest possible confidentiality.

If this factsheet has reassured you of our secure handling of your sustainability plans, we invite you to **join Data Safe House**. Because the more companies participate, the faster grid operators can build the new energy infrastructure. Together, we can accelerate the energy transition!

Join us and share your sustainability plans in Data Safe House!