Data processing Agreement

1. Introduction - definition of roles - applicability of this Data processing agreement

This Data Processing Agreement is an Addendum to the Platform' s Terms and Conditions of Use to which is an integral part, entered into by the EnergyGuard Consortium Partners (herein EnergyGuard, listed in Platform's Privacy Policy) and the External-User (as defined in the Platform's Terms and Conditions of Use), as of the effective date referred therein. The present Data Processing Agreement (herein after "DPA") is necessary since according to the EnergyGuard Platform Data Protection Notice/Privacy Policy https://dashboard.energy-guard.eu/static/assets/docs/privacy-policy.pdf for any Platform feature that needs input data from the External-User to function or enables the External-User to add datasets, that contain personal information (related to the External-User of other data subjects), the External-User/TEF tester act as the Data Controller for such data, although uploading personal data in the Platform should be avoided. In such cases, the External-User remains solely responsible for his/her compliance with his/her data protection obligations laid down by data protection legislation as a Controller, and the Platform's Administrator and the rest of Consortium partners process this data solely on your behalf acting as Data Processors. In this case the terms included herein regarding the processing of personal data by EnergyGuard as data processor on behalf of you as the Controller apply. With regards to the processing operations related to the Platform, for which EnergyGuard is the Data Controller, the EnergyGuard Platform Data Protection Notice/Privacy Policy https://dashboard.energy-guard.eu/static/assets/docs/privacy-policy.pdf applies.
More specifically, the present DPA applies to the processing of those data/datasets uploaded/added/stored to the EnergyGuard Platform by the External-User, produced and processed on the basis of the External-User's use of Platform regulated by the Terms and Conditions of Use, that include personal data, in order for the External-User to test, validate, experiment with and evaluate Artificial Intelligence (AI) solutions in the energy sector through the Use of EnergyGuard Platform/tools and functionalities. The present DPA is without prejudice to any other External-User obligations being activated on the basis of other non-personal data use or sharing.

2. Obligations of the parties:

2.1 EnergyGuard obligations

2.1.1 EnegyGuard processes External-User's personal data only on External-User's documented instructions (including those that are defined herein and in the Terms and Conditions of Use), unless EnergyGuard is required to do so by law, to which it is subject. This includes transfers of personal data to a third country or international organisation. In case EnergyGuard considers that an External-User's instruction infringes GDPR or other applicable data protection legislation, it will immediately inform the External-User and abstain from any further processing action based on this instruction until the instruction is appropriately modified/corrected. In case EnergyGuard is required by law to process data without documented instructions from the External-User, it will inform the External-User of that requirement within reasonable time before processing, unless it is legally prohibited to provide such information on important grounds of public interest. In case EnergyGuard becomes aware of any External User's processing/action that may infringe Data Protection Legislation, EnergyGuard is entitled to suspend or terminate an External-User's access to the Platform or use.

2.1.2 EnergyGuard ensures that persons that are authorized to process personal data (e.g employees of Consortium Partners or other collaborators) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

2.1.3 EnergyGuard implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk that the processing of External-User's personal data may have to the rights and freedoms of natural persons in accordance with Data Protection Legislation. These measures are listed in Appendix B of the present. The External-User, after being informed of the measures implemented by EnergyGuard, he/she acknowledges them as appropriate to ensure a level of security appropriate to the risk in compliance with the applicable data protection legislation.

2.1.4 When applicable, the External-User provides herein EnergyGuard a prior and general authorization to engage Sub processors to carry out specific processing activities related to the Platform and to the processing that takes place according to the present. In such case an updated list of Sub processors will be available in the Website. In case of intended amendments/replacement to the Sub-processors, the External-User will be appropriately informed prior to their engagement and an exclusive deadline of 5 days to provide his/her written reasonable objections (through e mail at privacy@energy-guard.eu) related to personal data legislation related issues will initiate. After the passing of that date, if no objection is raised by the External-User, the new Sub-Processors will be deemed approved. In case of engagement of a Sub processor for carrying out specific processing activities (on behalf of the External-User), EnergyGuard shall bind the Sub processor with a written agreement that includes the same data protection obligations as the ones referred herein. At the External-User's request EnergyGuard may provide a copy of the sub-processor agreement. To the extent necessary to protect business secrets or other confidential information, EnergyGuard is entitled to redact parts of the text of the agreement prior to sharing a copy to the External-User. In case objections to the engagement of a Sub processor are raised by the External-user, EnergyGuard is entitled to propose other Subprocessor, to undertake itself to execute that processing or to interrupt the Use of the Platform for this specific External User by informing the External User that the provision of services cannot take place without the use of the specific Sub-Processor.

2.1.5 The EnergyGuard, taking into account the nature of processing shall provide reasonable assistance to the External-User by appropriate technical and organizational measures to the extent possible and commercially feasible, in order for the External-User to comply with his/her obligations to respond to data subject's requests to exercise of their rights laid down by the Data Protection Legislation. In case a data subject submits its request for the exercise of his/her rights directly to the EnergyGuard, the later will notify the External-User without undue delay so as for the External-User to appropriately address the request within the deadline provided by Data Protection Legislation. The External-User is exclusively liable for the lawful management and satisfaction of data subject's rights in compliance with Data Protection Legislation. EnergyGuard will not take any action to address data subject's rights unless this consists its own legal obligation.

2.1.6 EnergyGuard, taking into account the nature of the processing and the information available, following External-User's written request (through e-mail), to the extent reasonable according to the nature of the processing and the processor's involvement in it, will assist the External-User to ensure compliance with his/her obligations laid down by the GDPR related to the security of personal data processing, the notification of personal data breach to the supervisory authority, the communication of a personal data breach to the data subject, the conduct of a data protection impact assessment and the prior consultation with the supervisory authority when required by law. In case of a data breach, the External-User will be notified by EnergyGuard after the later becomes aware of the breach without undue delay. Such a notification shall not be construed as an acknowledgment of fault or liability regarding the Data Breach by EnergyGuard. The External-User shall notify the result of the audit to EnergyGuard. The External-User is solely liable for taking the decision to notify the data breach to the supervisory authority and/ or data subjects with regards to personal data being

processed under the present data processing agreement, in which case he/she should prior to the notification inform EnergyGuard of its content, in case there is reference to it in the notification.

2.1.7 After the end of the use of the Platform, EnergyGuard shall delete or return all personal data to the External-User unless applicable EU or State law requires storage of personal data or in case otherwise agreed between the External-User and EnergyGuard.

2.1.8 To the extent possible and applicable to the operation of the Platform, EnergyGuard shall provide the External-User with the reasonably necessary information to demonstrate his/her compliance with the obligations provided herein, subject to confidentiality and trade secrets protection of EnergyGuard and its partners. Audits in the infrastructure and systems of EnergyGuard (maximum volume of audits permitted: one per year or after a request by supervisory or other appropriate authority) are permitted only to the extent that information requested by the External-User is not already provided to the External-User otherwise. Audits are permitted only after providing a prior notice to EnergyGuard (through email at privacy@energy-guard.eu) at least 60 days prior to the audit. The audit can be conducted only by persons that are strictly bound to confidentiality obligations, are not competitors to EnergyGuard and it should be restricted to data processing relating to the specific External-User and should not impede EnergyGuard's proper business continuity and other legitimate commercial/research interests. The External-User acknowledges and hereby provides his/her consent to EnergyGuard to permit audits/inspections or other type of reviews from the Funding Authority that may need access to their datasets, for purposes related to the funding procedure or where otherwise necessary by the applicable legislation.

2.1.9 EnergyGuard prioritizes processing of personal data within EEA, thus data processing takes place mainly within EEA. In case personal data are processed outside the EEA, EnergyGuard ensures that such processing takes place in accordance with the provisions of Chapter V of GDPR. Paragraph 2.1.4 applies to the extent applicable for the authorization of the Sub processors.

2.2 External-User's obligations:

2.2.1 External-User is obliged to comply with all obligations as a Data Controller under Data Protection Legislation, for the processing of personal data that takes place through his/her use of the EnergyGuard Platform in the scope of the present DPA.

2.2.2 External-User should, prior to uploading/adding datasets to the Platform, in order to comply with the principles of data minimization and to the extent possible, prioritize the use of anonymous and/or personal data that have undergone pseudonymization and implement measures to restrict the volume of personal data included in the datasets as well as to remove irrelevant personal data.

2.2.3 External-User is obliged to provide EnergyGuard with lawful instructions for the processing of personal data that takes place through his/her Use of the Platform.

2.2.4 External-User is solely and fully liable to provide data subjects whose personal data may be included in the datasets added/uploaded/processed through his/her use of the EnergyGuard Platform, the necessary and lawful prior information notice for that processing and obtain all necessary consents (if necessary) or use other lawful legal bases according to the personal data processing and purpose in compliance with Data Protection Legislation and all other legislation applicable for EnergyGuard to be able to legitimately process personal data through the Platform, according to this Data Processing Agreement and in compliance with Data Protection Legislation or any other Legislation applicable.

2.2.5 The External-User is solely and exclusively responsible for his/her compliance with data protection legislation or any other applicable legislation for the processing of the personal data that it adds/uploads to the Platform. The external-User is liable for any damage that may be caused to EnergyGuard and/or any third person/data subject (including among others,

complaints, claims or demands for compensation for any type of damage/injury and/or any other penalty incurred to EnergyGuard, EnergyGuard Partners or their collaborators related to the operation of the Platform by a supervisory authority), as a result of his/her infringement of his/her obligations laid down in Data protection Legislation related to any processing of personal data that falls within the scope of the present DPA through External-User's use of EnergyGuard Platform and from processing of personal data provided by the External-User through the use of the Platform. Article 14 of the Terms and Conditions of Use regarding Indemnification and User's Liabilities applies.

3. Final provisions

3.1 For the rest of the issues not specifically regulated herein as well as for any disputes or liabilities related to the present DPA, the provision of the Terms and Conditions of Use apply accordingly.

Appendix A – Description of Processing

Subject matter – purpose of the processing: to enable External-user to test and validate the AI applications submitted by him/her to EnergyGuard, through the use of the Platform and its functionalities

Duration of the processing: During the Platform's use from the External-User

Nature of the processing: includes at least collection, organization, structuring storage, retrieval, use, combination, restriction, erasure of personal data

Type of personal data: personal data included in the datasets uploaded/added by the External- User. Personal data included in the usage data and outputs of the External User's testing.

Categories of data subjects: data subjects related to the personal data included in the datasets uploaded and the relevant testing performed on such datasets.

Appendix B

Technical and organizational measures

Measures of pseudonymisation and encryption of personal data

Datasets uploaded can pseudonymized where feasible, separating direct identifiers from the underlying analytical data utilising anonymisation tools including Amnesia (https://amnesia.openaire.eu/), ARX tool https://arx.deidentifier.org/ and traditional anonymization using Pandas DataFrames. Transmission of the data over public networks is encrypted using strong cryptographic protocols (e.g., HTTPS, TLS 1.2 or higher)

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Strict Role-Based Access Control (RBAC) is enforced to the management of the uploaded data. Access to processing systems is granted on a "need-to-know" and "least privilege" basis. Incoming data manipulation are automatically distributed across multiple healthy servers to prevent performance bottlenecks using NGINX. Core processing environments utilize redundant, high-availability cloud architecture with automated failover capabilities to ensure continuous operation of intelligent measurement systems.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Automated, encrypted backups of all critical databases and configuration files are performed on a daily basis using Microsoft Hyper-V as well Microsoft's native VSS (Volume Shadow Copy Service)

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Automated vulnerability scanning is conducted quarterly on all external-facing applications, APIs, and infrastructure. Penetration Testing Independent third-party penetration testing is conducted on core platforms at least annually. Security Audits: Internal reviews of access logs, system configurations, and security policies are conducted on a regular cadence.

Measures for user identification and authorisation

Complex password requirements (minimum length, character variety) and regular forced resets are enforced. Keycloak is used as a decentralised Identity and Access Management (IAM) system to provision, modify, and promptly revoke user access per dataset upon termination or role change.

Measures for the protection of data during transmission

Firewalls, intrusion detection/prevention systems (IDS/IPS), and Virtual Private Networks (VPNs) are utilized to secure data perimeters and internal network segments. Deprecated or insecure communication protocols (e.g., Telnet, unencrypted FTP) are strictly prohibited.

Measures for the protection of data during storage

Client data and multi-tenant environments are logically segregated to prevent unauthorized access or data leakage between different datasets in the environment of Minio, MLFlow and JypyterHub.

Measures for ensuring physical security of locations at which personal data are processed

Primary data processing and storage occur in a secure facility compliant with ISO 27001 and SOC 2 Type II, featuring 24/7 security, access controls, and environmental safeguards.

Measures for ensuring events logging

Wazuh, a Security Information and Event Management (SIEM) system, is used to aggregate and correlate logs from the infrastructure the datasets reside. Audit Trails: Immutable audit logs are maintained for user logins, administrative actions, privilege changes, and access to personal data, retained for a minimum of 90 days.

Measures for ensuring system configuration, including default configuration

Hardening: Servers, edge devices, and networking equipment are configured according to industry-standard hardening baselines (e.g., CIS Benchmarks). Privacy by Default: New system deployments and intelligent processing platforms are configured with the most privacy-restrictive settings enabled by default.

Measures for internal IT and IT security governance and management

Comprehensive Information Security Policies are documented, endorsed by management, and made available to all personnel. All employees and contractors undergo mandatory security awareness and data protection training upon hire and annually thereafter.

Measures for certification/assurance of processes and products

The infrastructure of dataset management is currently being hosted on our information Security Management System (ISMS) which was officially certified adhering to the ISO 27001:2022 standard.

Measures for ensuring data minimisation

The platform is configured to notify the user about utilising data strictly necessary for the defined processing and AI experimentation and validation purposes. A dynamic size limit is enforced to the data uploaded by the users

Measures for ensuring data quality

The platform parses all incoming datasets (e.g., CSV, JSON) upon ingestion to verify structural integrity. This includes confirming recognized file formats, correct delimiter usage, proper field alignment, and automatically rejecting corrupted, incomplete, or malformed files before processing begins.

Measures for ensuring limited data retention

The platform enforces automated retention policies. Uploaded datasets are actively retained only for the duration of the defined processing purpose, not exceeding 24 months. Upon expiration of the retention period, automated scripts execute the secure deletion of the datasets. Data residing in secure system backups or disaster recovery archives is naturally overwritten or destroyed in accordance with a strict backup rotation schedule, not exceeding 90 days

Measures for ensuring accountability

Regular internal audits are conducted to verify adherence to documented security policies. All personnel with access to the processing environment undergo mandatory, documented data privacy and security training annually

Measures for allowing data portability and ensuring erasure

The platform provides self-service export functionalities and dedicated APIs that allow users to securely extract their uploaded datasets and generated insights in structured, commonly used, and machine-readable formats (e.g., CSV, JSON) or to be uploaded to code repositories such as github / gitlab.