This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 893240

DELIVERABLE

Project Acronym: REScoopVPP

Grant Agreement number: 893240

Project Title: Smart Building Ecosystem for Energy Communities

---

D.7.3 Data Protection Approach

Revision: version 1

Authors:

Roland Tual (RESC)

Sara Tachelet (RESC)

Jan Pecinovsky (EID)

.....

REVISION HISTORY AND STATEMENT OF ORIGINALITY

Revision History

Revision	Date	Author	Organization	Description
V. 0.1	07.10.20	Roland, Jan, Sara	RESC	Outcome of the first f2f meeting
V. 0.2	02.12.20	Roland	RESC	Updated version with partner notifications for complementary details needed
v.0.3	07.12.20	Roland	RESC	Finalisation 1st draft with notifications for partners to review
v.0.4	11.12.20	Roland	RESC	Meeting with concerned partners and discussion on pending issues
v.1	17.12.20	Roland	RESC	Inclusion of all partner comments
v.1.1	21.12.20	Manuel	SNAP	Peer Review

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Executive Summary

The objective of the REScoopVPP project is to create the most advanced community-driven smart building ecosystem for energy communities. The ecosystem consists of a Community-driven Flexibility Box (COFY-Box) acting as smart home controller, and a set of community tools to support energy services for aggregators, ESCO's, BRP's and suppliers of RES. The COFY-box together with the Community tools will enable energy communities to become real-time asset operators by employing demand and production forecasting algorithms, a dynamic pricing module for implicit Demand Response and an OpenADR-based explicit Demand Response solution.

This deliverable highlights the REScoopVPP chosen approach to ensure data security and data privacy towards data subjects, based on the requirements of the GDPR [3]. REScoopVPP pilot end-users' rights as data subject will be addressed through a dedicated strategy. The chain of responsibility has been identified, pilot-sites cooperatives play the role of Data Controller and technical partners are Data Processors. This relation will be made more tangible through the implementation of contractual relationships using explicit consent between pilot end-users and pilot cooperatives and a data processing agreement between pilot cooperatives and technical partners. Being a rather small-scale project, it appears that REScoopVPP does not require a Data Protection Officer, however the present document includes REScoopVPP Data Protection Assessment.

Energy consumption data and other personal data represent the key resource for the functioning of the REScoopVPP solution and the different services it enables. The processing purpose of each data type is described in this report, together with a brief explanation on the scope and context of the data processing for the different functionalities of the solution. A high-level view on the REScoopVPP main data processing activities is provided together with a diagram illustrating data flow and personal data processing. A light is shed on the different REScoopVPP components, the related project partner operating each of them, the personal data being processed in this component, their collection frequency and storage period.

The measures to protect personal data are presented both from an architecture point of view, identifying the different assets (hardware, software, networks, people, paper or paper transmission channels) which are physically supporting the data processing for each component; and in a more holistic way, with an overview represents of planned measures (data minimisation; state of the art authentication and consent; limited and pseudonymised access for R&D; no CRM data access to data processors).

Finally the consortium committed to respect the following key principles in order to safeguard data subject's rights: appropriate information; informed explicit consent; preventive measures for sensitive data; processing limited to project purpose, data minimisation, deletion of shadow data and ensuring confidentiality.

Table of content

Abbreviations

BRP Balance responsible Party

CRM Customer Relationship Management

DPA Data Protection Approach (the current deliverable)

DPIA Data Protection Impact Assessment

DPO Data Protection Officer

DR Demand response

ESCo Energy Service Company

GDPR General Data Protection Regulation

RES Renewable Energy Source

1. Introduction

The objective of the REScoopVPP project is to create the most advanced community-driven smart building ecosystem for energy communities. The ecosystem consists of a Community-driven Flexibility Box (COFY-Box) acting as smart home controller, and a set of community tools to support energy services for aggregators, ESCO's, BRP's and suppliers of RES. The COFY-box together with the Community tools will enable energy communities to become real-time asset operators by employing demand and production forecasting algorithms, a dynamic pricing module for implicit DR and an OpenADR-based explicit DR solution.

As announced in REScoopVPP description of activities, this deliverable highlights the REScoopVPP chosen approach to ensure data security and data privacy towards data subjects, based on the requirements of the GDPR [3]. This report describes how the roles of data controllers and data processors are handled within the consortium, together with a description of the data flow within REScoopVPP and the related protection measures taken.

The Data Privacy Approach describes how REScoopVPP partners will build products and services which comply with the requirements of the GDPR, and therefore ensure data security and data privacy towards data subjects. This report is distinct from the Data Management Plan included in D7.2 *Communication and Dissemination Plan* which addresses all data collected and used by REScoopVPP as a project.

The structure of the document is inspired from the Data Protection Impact Assessment (DPIA) for Smart Grid methodology proposed by the Expert Group 2 of the Smart Grids Task Force (SGTF-EG2) [1]. It complies with the first steps, providing a thorough description of the motivations for data processing, the involved parts of REScoopVPP architecture, the related partners and the protection measures. However the threat identification, risk assessment and following steps (steps 4,5 and 6) have been replaced by a thorough description of REScoopVPP chosen protection measures.

Finally, this deliverable includes relevant content for D9.1 and D9.2. The document contains relevant details regarding *D9.2 : POPD - Requirement No. 2*, including:

- REScoopVPP's decision regarding the appointment of a DPO;
- How all of the data they intend to process is relevant and limited to the purposes of the research project;
- A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants.

Regarding *D9.1 : H - Requirement No. 1*, the document includes:

- The informed consent procedures that will be implemented for the participation of pilot sites end-users;
- Templates of the informed consent/assent forms and information sheets to be translated by each pilot site into the local language);
- Clarifications on the participation of children and/or adults unable to give informed consent or vulnerable individuals/groups.

The procedures and criteria that will be used to identify/recruit research participants are not included in the present deliverable.

2. The GDPR Framework for Data Privacy

The article 4 of the General Data Protection Regulation (GDPR, [3]) introduces some essential concepts, which are introduced below together with their interpretation in the context of REScoopVPP.

2.1 Key concepts of the GDPR and their relevance in REScoopVPP

Personal data

GDPR definition: 'personal data' means: "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*"

The EG2 DPIA Template also provides some examples in its section 2.1.3. "Criterion 3 – Personal Data involved and DPIA – related Data Processing activities" p. 25-26.

In REScoopVPP, this may represent: name, address, contact details, information concerning the technical equipment present in a house, electricity consumption data or other consumer electricity consumption-related information together with possible contractual information.

Pseudonymisation

The 4 paragraphs below provide 3 key elements from the GDPR on pseudonymisation, together with the REScoopVPP chosen approach.

Definition (GDPR, art. 4) : **'pseudonymisation'** means: "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".

Pseudonymised data VS anonymous data (GDPR, recital 26): *"The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. (...)."'*

Pseudonymisation alone is not enough (GDPR, recital 28): *"The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and*

help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection. "

REScoopVPP approach. In REScoopVPP, pseudonymisation will be one of the core techniques applied. Pseudonymisation will be performed at pilot cooperatives level, prior to any further data processing. The information required to reverse the pseudonymisation will be accessible only to pilot cooperatives. This way, the different modules of the REScoopVPP solution will only process pseudonymised data.

Data Controller and Data Processor

The 4 paragraphs below provide 3 definitions from the GDPR on the role of controller and processor, together with the appointed related actors in the REScoopVPP .

Definition (i) (GDPR, art. 4): ***'controller'*** *means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State Law.*

Definition (ii) (ibid.): *'**processor'** means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller*

Definition (iii) (ibid.): ***'processing'*** *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

In REScoopVPP, the **Data Controllers** are the pilot cooperatives. They are providing access to their members' data and remain responsible in front of them for the use of these data in the context of the project. Data controllers may also engage in data processing activities, activities for which they remain responsible in front of the data subjects. These pilot cooperatives are:

- BE pilot: EnerGent
- DE pilot: Bürgewerke
- FR pilot: Enercoop
- ES pilot: Som Energia
- UK pilot: Carbon Co-op

The processors are all the technical partners who will use consumer data in order to build the REScoopVPP smart home services that will be offered by the pilot cooperative (data controllers). These technical partners are:

- EnergieID

- Carbon Co-op
- Gent University

Enercoop will not process personal data, but only aggregated and anonymous consumption data . These data from the pilot cooperatives will be treated confidentially.

2.2 The roles of Data Controller and Data Processor

Data controllers are the main responsible for the implementation of data subjects' rights. They are responsible for [2]:

- provisions setting for lawful processing;
- provisions on the rights of the data subjects, to information, access, rectification;
- erasure and blocking, and to object to the processing of personal data;
- provisions on notification and prior checking;
- possible damage resulting from unlawful processing.

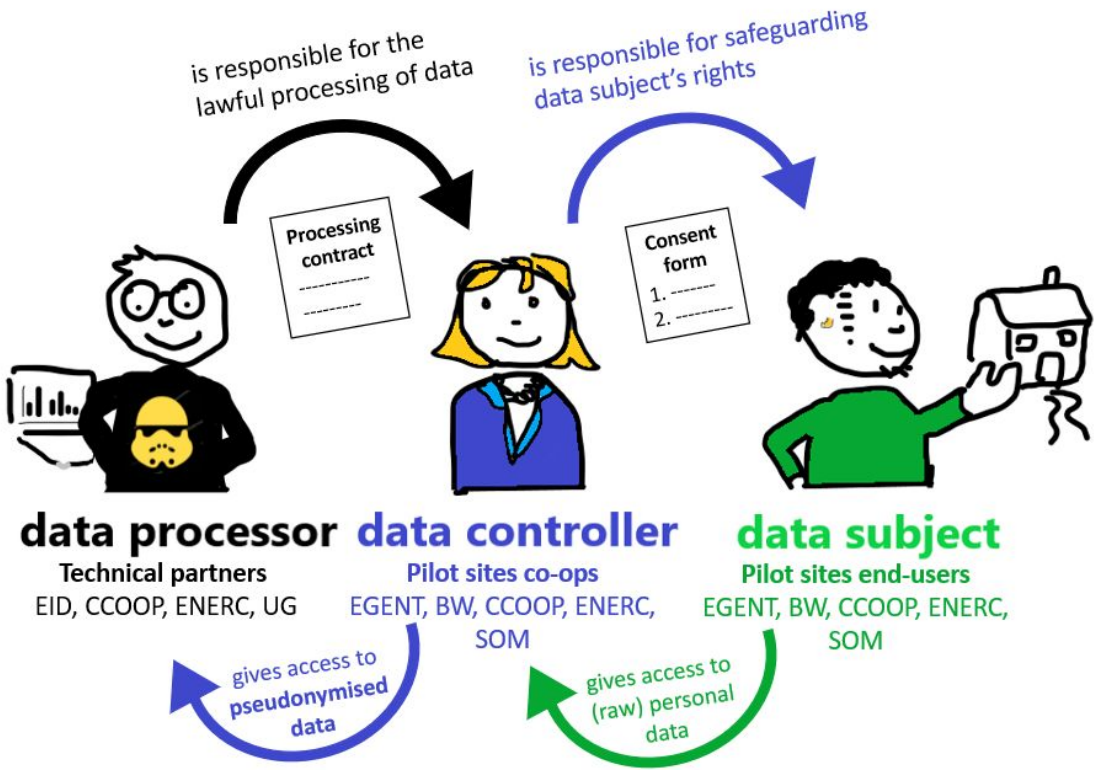
The controller "*must implement appropriate technical and organisational measures to protect personal data against* (…) *and against all other unlawful forms of processing*" (GDPR art. 17 (1)).

"[P]rocessing by a processor shall be governed by a contract or other legal act under Union or Member State law…" (GDPR, art. 18)

Responsibility chain in REScoopVPP. The Data Controller guarantees to data subjects that their data will only be used for the specific purpose agreed, in a secure manner, and with due respect to their data subjects' rights (right to correction, right to portability, right to be forgotten). These right will be formalised through 2 main sets of contracts:

· Contracts between controllers and end-users: a consent form to be signed by each end-users involved in the pilot (the template is available in *Annex 3: Template - Declaration of Consent in REScoopVPP);*

· Contract between controllers and processors, enabling controllers to guarantee rights are respected (the template is available in *Annex 4: Template - Contract between Data controller and data processor*)



2.3 The Data Protection Officer

According to the GDPR [3], a Data Protection Officer may be appointed in order to monitor the implementation of the data protection measures.

Need for a DPO (GDPR, art. 37): *1.The controller and the processor shall designate a data protection officer in any case where:*
(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

In REScoopVPP, (a) the consortium is not a public authority, (b) the regular and systematic monitoring of energy consumption data will only take place at a limited pilot scale: 50 (BE) + 20 (FR) + 25 (ES) + 50 (UK) = 145 homes + 5 Tertiary or multi-apartment buildings (DE); (c) the project does not involve the processing of special categories of data pursuant to Article 9 and personal data relating to criminal convictions. Therefore the appointment of a DPO does not appear required.

2.4 The Data Protection Impact Assessment

When data processing is likely to result in a high risk to the rights and freedoms of natural persons, the GDPR requires the use of a Data Protection Impact Assessment (DPIA). The DPIA is defined in Article 35 of the GDPR [3].

Content of the DPIA (GDPR, art. 35 (7)):*The assessment shall contain at least:*
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

REScoopVPP approach. In order to take consistent measures and to ensure efficient protection of REScoopVPP pilot end-users, the consortium has been conducting a DPIA. The different requirements (a), (b), (c) and (d) above can be found in the next section of this deliverable.

3. Data Summary

This section clarifies the general purpose of the project and therefore of data processing together with the specific purpose of each type of collected data.

3.1 Purpose of Data Generation and Relation to the Project

The REScoopVPP project combines front-runner energy communities to create the most advanced community-driven smart building ecosystem for energy communities. The ecosystem consists of a Community-driven Flexibility Box (COFY-Box) acting as smart home controller, and a set of community tools to support energy services for aggregators, energy services companies, balance responsible parties and suppliers of renewable energy source-electricity.

In this context, personal data (especially consumption) data will be recorded in order to enable the different features of the REScoopVPP solution: (i) giving end-users access to online energy monitoring tools; (ii) optimising self-consumption by piloting some residential appliances; (iii) enabling dynamic tariffs and the consumption of cheaper retail electricity; (iv) aggregating residential resources in order them to participate into explicit demand response services; (v) forecasting demand and generation to support these activities and other ones performed by energy cooperatives as supplier or ESCos.

For these purposes the processing of consumption and (on-site) generation data and of complementary energy or contextual information is needed. These information are detailed in the following section.

3.2 Data Types and Purposes

This section provides an overview of all data being collected and the purpose of their processing. It involves information only data controllers will have access to and information which will be transferred to data processors.

Cooperative pilot data (data controllers only)

Pilot cooperatives (Data controllers) will keep personnel information separately from the EScoopVPP solution. This includes end-user names, addresses and contact details; only pseudonyms will be shared with data processors.

Moreover, for the purposes of portfolio forecasting, pilot cooperatives will create a dataset containing the total load/production of their portfolio. Data should be aggregated and anonymous.

Related component	Personal data	Purpose
Pilot cooperative Client Relationship Management	● End-user name ● Address ● Contact details	Customer identification, communication channel and energy needs estimation. *Basic info already collected by the cooperative*
Pilot cooperative	● Yearly consumption ● Corresponding synthetic energy profile, or real load profile if available.	Load forecast calculation *This data will be aggregated, only anonymous data should be transferred to processors*

Technical partners data (data processors)

This section provides an overview of data being collected and the purpose of their processing by REScoopVPP tools.

Related component	Personal data	Purpose
COFY Box - Local	● High frequency, high resolution electricity data ● High frequency, high resolution heating data ● High Frequency, high resolution temperature measurement	Local monitoring, forecasting, control and optimisation of energy consumption, production and flexibility at house level only, e.g. self-consumption optimisation
	● List of available assets/ appliances ● Location ● Flexibility preferences	Context defining flexibility potential and limitations

	CoFy Box device diagnostic (incl. connectivity)	Maintenance
Cloud (digital twin)	• Minimised electricity data • Minimised heating data • Minimised temperature measurement	Measurement and verification of energy performance, follow-up of triggered flexibility activity (at cooperative level e.g. for dynamic pricing)
	• Cooperatives membership • Log-in credentials (incl. language preferences) • Sharing preference (who has access to data) • Access log (who accessed data)	Personalisation and services customisation
	CoFy Box device diagnostic (incl. connectivity)	Remote maintenance
cVPP system (shared)	• All digital twin data (above) with explicit consent • Clustered data (incl. cluster definition)	Measurement and verification of energy performance, follow-up of triggered flexibility activity (at third-party level, e.g. for independent aggregation purpose)
Portfolio forecasting tool	Anonymous aggregated data	Monitoring of aggregated energy behaviour to improve forecasting
	No further mention of the portfolio forecasting tool will be made since it does not process personal data	

4. Nature, scope, context and purposes of the processing in REScoopVPP

The REScoopVPP consortium aims at developing the services below. For each of them the context for data processing is detailed.

Giving end-users access to online energy monitoring tools:

- **Nature and scope**: COFY box and Cloud data (see table above) will be processed to be translated into graphs and other readable information.
- **Context and purpose**: processed data will be made available and visible directly to the end user through a web interface in order to facilitate energy efficiency actions.

Optimising self-consumption by piloting some residential appliances:

- **Nature and scope**: COFY box, Cloud data and cVPP data (see table above) will be processed to establish and update close-to-real-time individual consumption and generation profiles.
- **Context and purpose**: data will be processed in order to reschedule the operation of some home appliances in order to consume electricity at time of self-generation.

Enabling dynamic tariffs and the consumption of cheaper retail electricity:

- **Nature and scope**: COFY box, Cloud data and cVPP data (see table above) will be processed to establish and update close-to-real-time individual consumption and generation profiles. (*as above*)
- **Context and purpose**: data will be processed in order to reschedule the operation of some home appliances in order to consume electricity at times of low electricity prices on the wholesale market.

Aggregating residential resources in order to participate into explicit demand response services:

- **Nature and scope**: COFY box , Cloud data and cVPP data (see table above) will be processed to establish and update close-to-real-time individual consumption and generation profiles. (*as above*)
- **Context and purpose**: data will be processed in order to reschedule the operation of some home appliances in order to offer aggregated residential loads to third-party aggregators.

5. Functional description of the processing operation

The section below provides a high-level view on the REScoopVPP main data processing activities.

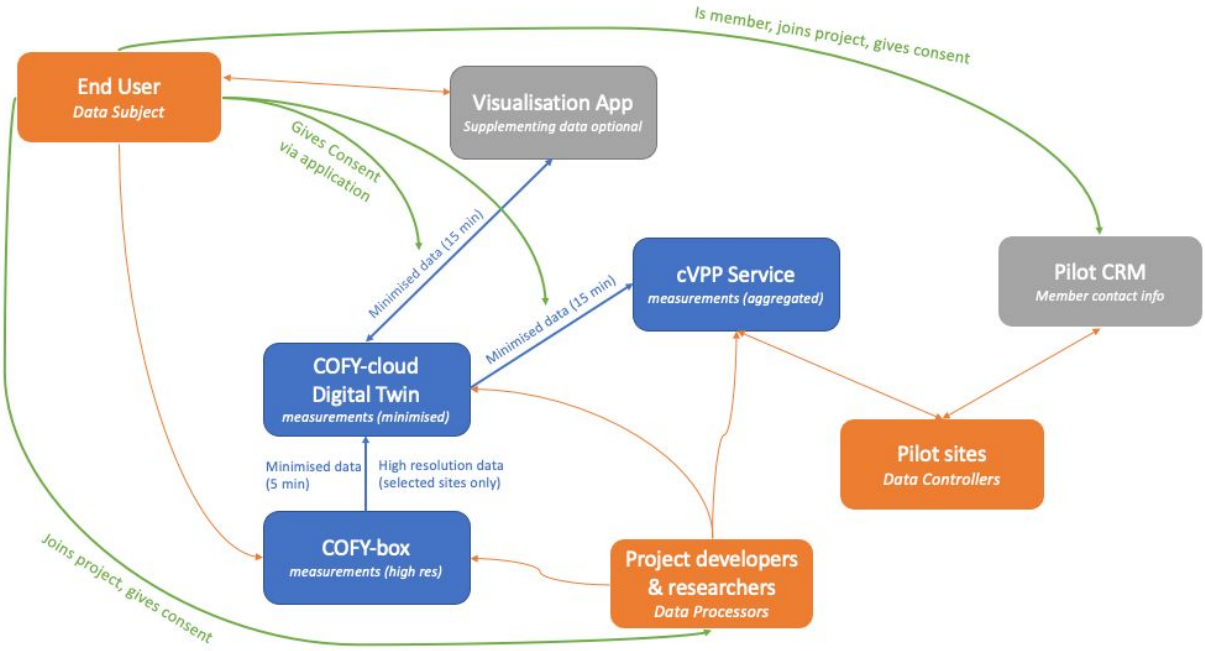
5.1 Processing Operation Overview

The section below describes the four main entries of private data together with a high-level description of the main related processes:

- **Contact details**: these personal data are collected by the pilot cooperatives and kept separately from the rest of the REScoopVPP tools. Only pseudonymised data will be passed on to the REScoopVPP tools and partners, except where explicit consent is given.
- **COFY Box**: Households data (see section *Data types and format* above) are being processed locally and transferred to the end-user platform for energy monitoring purposes.
- **User Log-in**: In order to log in to the online tools, any user will have to use a user account, characterized by a name and e-mail address.
- **Additional data from external data controllers**: End-users may be offered the possibility to supplement their energy data (data types identical as above) by sharing data from an external system with the REScoopVPP tools. An explicit consent from the data subject will be asked whenever such a sharing of data occurs.

5.2 REScoopVPP data flow, components and related data processors

The diagram below describes the path of private data throughout the REScoopVPP modules.



The **orange** boxes represent the 3 actors: Data Subject, Data Processors and Data Controllers.
The **orange** arrows represent the data access of these roles:

- Data subject has direct local access to the COFY-box
- Data subject has access to the data stored in the COFY-cloud Digital Twin, via an external Visualisation App.
- Data Processors have remote access to the COFY-boxes, the Digital Twins and the cVPP Service. All data is pseudonymised for these actors.
- Pilot Sites have access to the cVPP services, which gather data from COFY-boxes via their Digital Twins after consent from the Data Subject.
- Pilot Sites can link pseudonymised data from the cVPP Services to their members, via their internal CRM system.

The **blue** boxes represent the REScoopVPP tools: COFY-box, COFY-cloud Digital Twin and cVPP Services.
The **blue** arrows represent data exchanges between these tools:

- COFY-box uploads minimised data to the COFY-cloud Digital Twin. By default, this data is minimised to 5 minutes resolution.
- The COFY-cloud Digital Twin can share data with the cVPP Services and with External Visualisation Apps.

The **green** arrows represent the consent of the Data Subject:

- The Data Subject gives consent to a pilot site to retrieve data stored in the COFY-cloud Digital Twin via the cVPP Services, though an interface in the application.

- The Data Subject gives consent to an external application to retrieve data stored in the COFY-cloud Digital Twin, through an interface in the application. An additional consent can also be given to the REScoopVPP tools to retrieve information stored in that external application.
- The Data Subject gives consent to the Data Processors to access their data, through the Consent Declaration supplied by the project.
- The Data Subject gives consent to the Data Controller to link data from their CRM-system, through the Consent Declaration supplied by the project.

The **grey** boxes represent external applications where personal information may be stored, that are not controlled by the REScoopVPP project, but may be linked to the REScoopVPP tools.

6. Personal data, recipients and period for which the personal data that will be stored are recorded

The table below lists REScoopVPP different components, the related project partner operating it, the personal data being processed in this component, its collection frequency and storage period.

Recipients	**Component**	**Personal data**	**Collection frequency**	**Storage period**
Pilot site managers (and any technical partner which is mandated by the pilot site managers) Developers (EID, UG, CCOOP) End-users	**Co-Fy Box - Local**	High frequency electricity data High frequency heating data High Frequency temperature measurement List of available assets/ appliances CoFy Box device diagnostic (incl. connectivity) Location Flexibility preferences	Installer has access once Developers have remote access for improvement and maintenance End-users have constant access	Indefinite - as local storage permits Remote access for developers will be disabled once COFY-box is deemed stable enough and access is no longer needed.
End-users Developers (EID) Related co-op pilot site External parties with end-user's permission	**Cloud (digital twin)**	Minimised electricity data Minimised heating data Minimised temperature measurement Log-in credentials (incl. language preferences) Cooperatives membership	Default frequency = 5 minutes. Selected lab-pilots may have higher frequencies for in-depth analysis.	Information kept for 5 y. after the project for non-active users if requested by the European Commission (tbc). Storage indefinite for active users

Data owner = end-user		Sharing preference (who has access to data) Access log (who accessed data) CoFy Box device diagnostic (incl. connectivity)		Automatic deletion after 2 y. inactivity Access log and detailed device diagnostic will be kept for a limited period of 90 days.
Related co-op pilot site External parties with pilot sites' permission *Data owner = related pilot sites*	**cVPP system (shared)**	All digital twin data (above) with explicit consent Clustered data (incl. cluster definition)	Frequency = 5 min Clustered data aggregation performed on scheduled intervals.	*As above*

7. Assets on which personal data rely

This section aims at identifying the different assets (hardware, software, networks, people, paper or paper transmission channels) which are physically supporting the data processing for each component.

The present overview represents an anticipation of planned measures at M6. Updates will be included in the second iteration (M18). The final measures will be details in D6.4 Information Management and Security (M24)

7.1 COFY Box

The COFY box is an open and collaborative building controller, based on Raspberry Pi and using existing open source home automation technology.

Category	Related asset	Security measure
Hardware	Device capable of running the containerised Cofy software (standard: embedded Linux board, but users can supply their own device), internal memory storage (hard drive, SD card), external memory storage (external hard drive, USB thumb drive)	Physically only accessible by the user (on premises).
Software	Local database	Stored on local storage media accessible by the user only
	Configuration files	Not normally accessible remotely but access can be enabled by authorised persons for the sole purpose of providing technical support. Logs are streamed to device management platform but not stored or persisted.
	Logfiles	Logs are streamed to device management platform but are not stored or persisted beyond ~hours. Full logs are stored on device and only accessible to remote support staff for the purpose of providing technical support.

Networks	Local Area Network (WiFi, ethernet) Wide Area Network (WAN)	LAN: encryption used if supported by the connected equipment, network only locally accessible WAN: state of the art end-to-end encryption to cloud infrastructure
People	Local access: user, installer Remote access by developers/support staff (maintenance & upgrade): Remote access by flex service provider (devices automation):	Local access: only possible by LAN Remote access (maintenance): A period will be defined after which remote access is no longer needed, and all access methods will be removed. Remote access by service provider (devices automation): upon consumer consent, duly identified and without admin access.

7.2 COFY Cloud (digital twin)

The digital twin is one of REScoopVPP community tools. The digital twin is the key enabler supporting online access to data, for the end user and the pilot sites.

Category	**Related asset**	**Security measure**
Hardware	Databases and processes are hosted on a Platform as a Service (Microsoft Azure).	No physical access to hardware. Only selected personnel have administrator access.
Software	Data Access API Device Provisioning Service User Identity Service Data Storage Systems	External oAuth2 authentication is used, so no login-credentials saved on the system. Each device receives a unique and time-restricted key.
Networks	HTTPS	Services accessible via state of the art encrypted connection.
People	System Administrators	Developers use data from selected lab sites for most of their development. Researchers can request a pseudonymised data export, but have no direct access to the systems.

7.3 cVPP system

The cVPP system is one of REScoopVPP community tools. The cVPP system is the key enabler supporting pilot site views of aggregated and individual data.

Category	Related asset	Security measure
Hardware	Databases and processes are hosted on a Platform as a Service (Microsoft Azure).	No physical access to hardware. Only selected personnel have administrator access.
Software	Data Access API Data Storage Systems User Identity Service	External oAuth2 authentication is used, so no login-credentials saved on the system.
Networks	HTTPS	Services accessible via state of the art encrypted connection.
People	System administrators	Developers use data from selected lab sites for most of their development. Researchers can request a pseudonymised data export, but have no direct access to the systems.

8. Overview of privacy measures and assessment of risks

8.1 Overview of privacy measures

This section describes the key principles characterising REScoopVPP data protection approach.

1. Data minimisation

REScoopVPP actively aims to minimise the amount of personal data that is sent from the locally installed infrastructure towards the cloud. For the purposes of local control of equipment, a fast and highly detailed level of data is required, whereas visualisation and aggregation of energy data do not need all those details. By minimising data on the COFY-box, before they are uploaded, the risks of highly personal data falling into the wrong hands are vastly reduced.

2. State of the art authentication and consent

Users of the REScoopVPP tools, both end-users and pilot site employees, will be able to authenticate themselves using existing, state of the art identity services. This effectively removes the need of having to store log-in credentials in the tools, and can therefore not fall into the wrong hands.

3. Limited and pseudonymised access for R&D

Any personal data that is required for research and development purposes, is stored separately from identifying information (such as names, e-mail addresses, addresses etc.). Data processors that need personal data for R&D purposes can therefore access the data they need, without identifying info being revealed.

4. No CRM data access to data processors

In order to provide meaningful support for their participants, the pilot sites need access to identifying information about the participant. This information will be kept in the pilot site’s CRM-system, separated from the REScoopVPP tools. There may exist a one-way link between the REScoopVPP tools and the pilot’s CRM, enabling them to look up this information, but data processors will not be able to access these systems.

8.2 Assessment of risks

The table below provides a summary of the main risks and of how they have been addressed.

Category	Risk	Prevention
Hardware	Physical access to hardware	● Limiting physical access. ● Using servers with restricted administrator access.
Software	Third-party intrusion through direct connection Intrusion through authentication failure	● Limiting remote access (CoFy Box) ● State of the art authentication ● Data minimisation (Cloud and cVPP system)
Networks	Communication interception	● Pseudonymization ● Data minimisation (Cloud and cVPP system) ● Encrypted connections
People	Intrusion at processor side	● Pseudonymization ● Data Minimisation ● Duly secured IT access at processor side ● Limiting people with access

9. Ethics and Data Subjects Rights

As REScoopVPP partners committed to in the Grant Agreement, the following principles will be implemented. REScoopVPP will fully comply with all national legal and ethical requirements of the pilot site participating countries. Any data collection involving humans will be strictly held confidential at any time of the research. This means in detail that REScoopVPP will comply with the following principles.

Appropriate information. All the test subjects, and their legal guardians where applicable, will be informed and given the opportunity to provide their consent to any monitoring and data acquisition process that all the subjects will be strictly volunteers and all test volunteers receive detailed oral information.

Informed explicit consent. No data will be collected without the explicit informed consent of the individuals under observation and their legal guardian where applicable. This involves being open with participants about what they are involving themselves in and ensuring that they have agreed fully to the procedures/research being undertaken by giving their explicit consent.

Preventive measures for sensitive data. No personal or sensitive data will be centrally stored. In addition, data will be scrambled where possible and abstracted in a way that will not affect the final project outcome.

Data processing limited to project purpose. No data collected will be sold or used for any purposes other than the current project.

Data minimisation. A data minimisation policy will be adopted at all levels of the project and will be supervised by the Ethics Panel. This will ensure that no data which is not strictly necessary to the completion of the current study will be collected.

Deletion of shadow data. Any shadow (ancillary) personal data obtained during the course of the research will be immediately cancelled. However, the plan is to minimize this kind of ancillary data as much as possible. Special attention will also be paid to complying with the Council of Europe's Recommendation R(87)15 on the processing of personal data for police purposes, Art.2 : "*The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry*".

Ensuring confidentiality. Specific measures will be in place in order to protect the data subjects from a breach of privacy/confidentiality and any potential discrimination; In particular their names will not be made public and their participation will not be communicated to. Any incidental findings will be kept strictly confidential and erased from files under request from the enrolled subject.

The research to be conducted will be in full compliance with the principles and guidelines of "Ethics for Researchers" to Facilitate Research Excellence, prepared by the EC Governance and Ethics Unit in 2007.

10. Next steps related to Data Protection

The responsibility for data protection involves most partners of the REScoopVPP project.

Data processors (UG, EID, CCOOP)

- will keep on implementing data protection measures within the architecture of the REScoopVPP tools. An overview of such measures will be made available in *D6.4 Information management and Security*;
- Will commit themselves to lawfully process personal data and fully respect data subjects rights through the Data processing forms to be signed with data controllers.

Data controllers (EGENT, CCOOP, BW, SOM, ENERC)

- Will engage with end-users and select demo-sites participants while respecting their data subjects rights.;
- Review and translate Consent form to be signed by end-users and ensure themselves that the agreements are compliant with national laws.

The timetable below provides an overview of the different Data Protection Approach versions publications and related deliverables including relevant content for DPA updates.

Date	**Relevant milestone or deliverable**
M6 (November 2020)	**D7.3 Data Protection Approach**
M8 (January 2021)	D7.4 Dissemination and Communication Plan *(Including the Data Management Plan clarifying the management of research data within the project)*
M12 (May 2021)	*MS2 Flexibility of Legacy Equipment* *(information on data collection frequency and data retention needed for local control)*
M9 (February 2021)	*MS3 Final Specifications of the CoFy Box* *(implemented collection and storage characteristics)*
M24 (May 2022)	D6.4 Information Management and Security

11. References

[1] Smart Grid Task Force 2012-14, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems", 2018. Available at: https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

[2] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concept of "controller" and "processor"*, February 2010. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

[3] Regulation (EU) 2016/679 of the European Parliament and of the European Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Annex I - Declaration of Consent (template)

The declaration below aims at informing pilot site participants on their rights as data subjects and obtaining their explicit and informed consent. It will be translated into the local language and adapted by the pilot partners in order to comply with national regulation.

Declaration of Consent

This data collection is part of research activities within the larger context of a research project from the Energy field named **REScoopVPP**, co-funded by the European Commission under the Horizon 2020 Programme under Grant Agreement No. 893240. The research to be conducted aims to be in full compliance with the General Data Protection Regulation (GDPR).

Purpose of Research: The REScoopVPP project combines front-runner energy cooperatives to create the most advanced community-driven smart building ecosystem for energy communities. The ecosystem consists of a Community-driven Flexibility Box (COFY-Box) acting as smart home controller, and a set of community tools to support energy services for aggregators, energy service companies, balance responsible parties and suppliers of renewable energy source-electricity. Community tools will enable energy communities to become real-time asset operators by employing demand and production forecasting algorithms, a dynamic pricing module and an explicit demand response solution.

REScoopVPP solutions will undergo a large-scale experimentation in Belgium, France, Germany, Spain and the UK. More information on the project's website: http://www.rescoopvpp.eu/.

Duration of the Research Activities: The Research Activities last from June 2020 to May 2023.

Risks or Inconveniences: No risks are foreseen. You are only requested to be available to participate. Some home appliances will be automated, tests and adjustments may be performed along the project.

Privacy and Confidentiality: The project partners will collect user-related data for the installation, the running and fine-tuning of the REScoopVPP tools. As a voluntary participant in the REScoopVPP pilot sites experiments and analyses, personal data will be recorded: responses you may give in questionnaires, as well as your consumption data and other appliances usage related information. Recorded data will not include any personal identification.

The consortium will have to comply with all European and national legislation relevant to the country where the data collections are taking place. To this end:

- personal data managed by REScoopVPP partners will be pseudonymised and stored in a form which does not permit identification of users without complementary kept separately.

- Data processing will be done in respect to the purposes for which the data is being collected.

Your decision to whether or not give your authorization for the use and diffusion of the information provided by you is completely voluntary.

Data access and storage: Information will be held and used on a pseudonymised basis only for the purpose of the project REScoopVPP. Consumption data and other appliance usage-related information will be held on servers hosted in the European Union (or in the UK for British pilots) for processing. Your raw data will be kept confidential and not disclosed to third parties. Appropriate protection will be given for personal data stored for longer periods for historical, statistical or scientific use.

Data usage: Information is processed during the phase of data analysis for the functioning of the REScoopVPP tools and overall solution and will be shown in project reports. The results of this investigation may be published in scientific journals or conferences and may be used in further studies. Data is sufficiently pseudonymised and aggregated to prevent any possibility of identifying specific data subjects. Reports on this study will not contain any personal data or data that could lead to the identification of a specific data subject.

Termination: After the end of the project the data will be only accessible to the European Commission, and for auditing purposes only, until a 5 year period has passed. After this period the data of all non-active users will be destroyed. The authorization for the use and access to this information is valid until the end of the study unless the user cancels it before.

All Research Participants have **the right** to quit the REScoopVPP experiments at any moment, have the right to leave the project and require the deletion of their data, without any consequences and have the right to be informed by the Data Controller about the type of processing their data. Also they have the right to access, correct and delete his/her data at any moment. You can also obtain information and ask for rectifying it. If you decide to exercise your rights, including the withdrawal from the project, please contact the persons below ('contact persons').

Benefits: The results of the REScoopVPP project and any improvement made to the solution during the project will benefit a cooperative project aiming at making available to citizens initiatives smart home tools facilitating the energy transition.

Contact persons: Your participation is voluntary, consent can be refused, and withdrawal is possible at any time per email to:

- *Name Surname (email: xxxx@xxxxx, phone +xxxxxxxx)* (data controller representative 1)*;*
- *Name Surname (email: xxxx@xxxxx, phone +xxxxxxxx)* (data controller representative 2)*;*

Declaration on consent: I hereby declare my consent my data may be conveyed and documented for the above stated purpose. I confirm that my participation is voluntary. I am aware that I may withdraw my consent for data processing, and therefore withdraw from the project, at any time.

_____ _____

Name of pilot site participant Location, Date

_____

Signature pilot Participant

Annex II - Contract between Data controller and data processor (template)

Data processing agreement
(hereinafter: the "Agreement")

BETWEEN

- ENERGIEID (ENERGIEID), established in POSTHOFLEI 3, BERCHEM 2600, Belgium, VAT number: BE0562861306, represented by Vincent Dierickx (President) and Diedrik Kuypers (Member of the Board)
- THE SOCIETY FOR THE REDUCTION OF CARBON LIMITED (CCOOP), established in c/o URBED, 10 Little Lever Street, MANCHESTER M1 1HR, United Kingdom, VAT number: GB144278311, represented by: _____
- ENERCOOP (ENERCOOP), established in RUE SARRETTE 48, PARIS CEDEX 14 75685, France, VAT number: FR10484223094, represented by: _____
- SOM ENERGIA SCCL (SOM), established in CALLE PIC DE PEGUERA 15 ESCALA B PISO 1 PORTA 16, GIRONA 17003, Spain, VAT number: ESF55091367, represented by: _____
- ECOPOWER (ECOPOWER), established in Posthoflei 3, Berchem 2600, Belgium, VAT number: BE0445389356, represented by: _____
- ENERGET (EGENT), established in SLACHTHUISSTRAAT 30, GENT 9000, Belgium, VAT number: BE0542998575, represented by: _____
- BURGERWERKE EG (BW), established in HANS BUNTE STRASSE 8 10, HEIDELBERG 69123, Germany, VAT number: DE293833520, represented by: _____
- UNIVERSITEIT GENT (UGent), established in SINT PIETERSNIEUWSTRAAT 25, GENT 9000, Belgium, VAT number: BE0248015142, represented by: _____

Hereinafter referred to as the Parties. Each a "Party", together referred to as the "Parties";
WHEREAS the Parties are involved into the Horizon 2020 research project REScoopVPP, (hereinafter: "Project"), as governed by the Grant Agreement 893240, concluded between the Parties;
WHEREAS the Project necessarily implies the processing of certain personal data as defined under Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter: "GDPR"); whereas all parties in the Project have been designated in the Project Grant Agreement as data controllers as defined under the GDPR;

WHEREAS the Parties are therefore legally required to conclude a data processing agreement establishing each other's responsibilities within the framework of the Project;
WHEREAS the Parties are divided into two sets of roles and responsibilities. EID, CCOOP and UGent are Data Processors; ENERCOOP, EGENT, ECOPOWER, CCOOP, BW and SOM are Data Controllers for their respective pilot sites.

IT IS AGREED AS FOLLOWS:
1. Definitions and Interpretation
1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement;

1.1.2 "Personal Data" means any personal data processed by a contracted Data Processor on behalf of the Data Controller pursuant to or in connection with the Principal Agreement;

1.1.3 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.4 "EEA" means the European Economic Area;

1.1.5 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.6 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.7 "Data Transfer" means:

1.1.7.1 a transfer of Personal Data from the to a Data Processor; or

1.1.7.2 an onward transfer of Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.8 "Services" means the Project related-services the Data Controller provides in the frame of the Project's pilot.

1.1.9 "Subprocessor" means any person appointed by or on behalf of the Contracted Processor to process Personal Data on behalf of the Data Controller in connection with the Agreement.

1.1.10 “Project” means the REScoopVPP project, funded by the European Union’s Horizon 2020 research and innovation programme under the grant agreement No 893240.

1.2 The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Personal Data

2.1 Data Processors shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Personal Data; and

2.1.2 not process Personal Data other than on the relevant Project’s documented instructions, in particular in the Project’s grant agreement;

2.2 The Project’s documents instruct the Data Processors to process Personal Data.

3. Processor Personnel

Data Processors shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Data Processor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual’s duties to the Data Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processors shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Data Processor shall take into account the risks that are presented by Processing, in particular from a Personal Data breach.

5. Subprocessing

5.1 Data Processors shall not appoint (or disclose any Personal Data to) any Subprocessor unless required or authorized by the Data Controllers.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Data Processors shall assist the Data Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controllers obligations, as reasonably understood by the Data Controllers, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify the Data Controllers if they receive a request from a Data Subject under any Data Protection Law in respect of the Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of the Data Controllers or as required by Applicable Laws to which the Data Processor is subject, in which case the Processors shall to the extent permitted by Applicable Laws inform the Data Controllers of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Data Processors shall notify the Data Controllers without undue delay upon Data Processors becoming aware of a Personal Data Breach affecting Personal Data, providing the Data Controllers with sufficient information to allow the Data Controllers to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Data Processors shall cooperate with the Data Controllers and take reasonable commercial steps as are directed by the Data Controllers to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation Processor

8.1 The Data Protection Impact Assessment shall provide reasonable assistance to the Data Controllers with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Data Controllers reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Data Processors.

9. Deletion or return of Personal Data

9.1 Subject to this section 9 Data Processors shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Personal Data.

10. Audit rights

10.1 Subject to this section 10, Data Processor shall make available to the Data Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Data Controllers or an auditor mandated by the Data Controllers in relation to the Processing of the Personal Data by the Data Processors.

10.2 Information and audit rights of the Data Controllers only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Data Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Data Controller. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of Belgium.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the jurisdiction of the courts of Belgium.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Date:

- ENERGIEID (ENERGIEID), represented by Vincent Dierickx (President) and Diedrik Kuypers (Member of the Board)

  Date and signature:

- THE SOCIETY FOR THE REDUCTION OF CARBON LIMITED (CCOOP), represented by: _____

  Date and signature:

- ENERCOOP (ENERCOOP), represented by: _____

  Date and signature:

- SOM ENERGIA SCCL (SOM), represented by: _____

  Date and signature:

- ECOPOWER (ECOPOWER), represented by: _____

  Date and signature:

- ENERGET (EGENT), represented by: _____

  Date and signature:

- BURGERWERKE EG (BW), represented by: _____

  Date and signature:

- UNIVERSITEIT GENT (UGent), represented by: _____

  Date and signature: