mini
GHENT
UNIVERSITY

DATA TRANSFER AGREEMENT

with GDPR Special Terms (Separate Controllers)

A22/TT/2295

This data transfer agreement (the "Agreement") is entered into force on 14 December 2022 by and between the following parties:

Universiteit Gent (Ghent University), public institution with legal personality, having its administrative offices in Belgium, B-9000 Gent, Sint-Pietersnieuwstraat 25, company registration number 0248.015.142 **("UGent"** or **"Recipiënt")**

AND

Fluvius System Operator cv, having its offices at Brusselsesteenweg 199, 9900 Melle, Belgium, company registration number 0477.445.084 **("Provider")**

Start Date: 15 December 2022 **Term:** 5 years

Provider owns/controls the **Data** as described in the **Technical Annex** and Controls certain valuable technical and proprietary Information relating to these Data;

Recipiënt wants to obtain access to these Data for the use in the **Research** as described in the Technical Annex and Provider is willing to provide Recipiënt access to the Data which Recipiënt is willing to accept under the General Terms set forth in this Agreement;

The Data may contain or contain personal data as defined in European Regulation 2016/679 of 27 April 2016 concerning the protection of natural persons with respect to the processing of personal data and the free movement of data and until the repeal of Regulation 95/46/EC (hereinafter the **"GDPR");** in addition to the General Terms, the Special Terms relating to the storage, handling and processing of personal data ("Special Terms") are applicable to this Agreement.

This Agreement consists of this **Signing Page,** the **Technical Annex** and the **Special Terms.** In case of conflict between these documents, the Special Terms shall take precedence.

This Agreement constitutes the entire agreement between the parties and supersedes all prior arrangements, understandings, representations and Communications, oral or written with respect to its subject matter.

For Provider Fluvius

For Universiteit Gent (Ghent University)
Signature:

-- END OF SIGNING PAGE --

TECHNICAL ANNEX

THE DATA (description)

Code	Description	Technical Format
	Consumption data whose key to individual Identification (the EAN number) remains with Fluvius and is not accessible to UGent researchers. Additional metadata, like ownership of assets, date of first grid connection of PV or batteries, etc. Access to the data (a local UGent server or data storage, or in the cloud) is only possible with a password.	Format will be 'parquet' a Standard big data format used in Microsoft Azure.

The following aspects and related Information of the Data are considered to be confidential by Provider: identity, structure, characteristics, conformation, origin and properties of the Data, the uses to which it is or may be put.

RESEARCH- PURPOSE- RESTRICTED USE

Describe the Research on the Data - this is the purpose to which the use of the Data is restricted.

Scientific research about the electricity and gas consumption profile and the price elasticity of different consumer groups. We study in particular how consumers' consumption patterns change over time due to the installation of technologies (heat pumps, electric cars, batteries) and changes in prices, tariffs, and policy decisions."

-- END OF TECHNICAL ANNEX -

SPECiAL TERMS - STORAGE, HANDLING AND PROCESSING OF PERSONAL DATA.

As Between the parties as identified in the Data Transfer Agreement **A22-TT-2295** (the **"DTA")**

This Addendum is an integral part of the DTA; its provisions take precedence over the General Terms. All terms defined in the DTA shali have the same meaning in this Addendum. For the Purpose of this Addendum, both the Provider and the Recipiënt as identified in the DTA shali be referred to as the **"Controllers".**

In view of the fact that:

The Parties wish to set out their rights and obligations with respect to the protection of personal data as stipulated in European Regulation 2016/679 of 27 April 2016 concerning the protection of natural persons with respect to the processing of personal data and the free movement of data and until the repeal of Regulation 95/46/EC (hereinafter the "GDPR") and in the Act of 30 July 2018 on the protection of natural persons with respect to the processing of personal data (hereinafter the **"Privacy Act")** in the current addendum (hereinafter the **'Addendum').** As such they also wish to comply with the obligation to conclude a protocol on the electronic communication of personal data in accordance with Article 8 §1 of the Decree of 18 July 2008 on electronic administrative data traffic. This document will be published on the websites of both parties.

The terms used in this Addendum have the same meaning as defined in the GDPR and the Privacy Act;

Within the framework of the DTA, the Recipiënt may receive and process specific personal data that has been supplied by the Provider.

The Parties representto being informed and knowledgeable about UGent's General Data Protection Policy, in particular the "Generic Code of Conduct for the processing of personal data and confidential Information at Ghent University" as published on the UGent website; UGent shali provide a copy of these document upon first request.

The Data Protection Officer of Fluvius provided his advice on the draft of this agreement on 07/02/2023.

The Data Protection Officer of UGent provided his/her advice on the draft of this agreement on 31/01/2023.

1. SUBJECT

1.1. Recipiënt will only process personal data made available by or through the Provider within the performance of the DTA. Recipiënt will not process personal data for any other purpose, unless subject to deviating legal obligations. Recipiënt may only process the personal data of data subjects that the Provider has obtained on the basis of legitimate legal grounds and for legitimate purposes.

1.2. The Provider will make the following categories of personal data available to the Recipiënt (non-exhaustive list):

a) Energy consumption data: active 15 minute values

1.3. The personal data made available to UGent by the Controller comprise the following categories of data subjects (non-exhaustive list):

a) Clients: all Fluvius clients with a digital meter

1.4. The personal data will be made available periodically, namely 3 times, in January, July and November, because the capacity tariff is active since the first of January 2023 and it is important to be able to evaluate (1) a change in behaviour of the data subjects and (2) if this change in behaviour persists..

The communication of the personal data will be done for a period from beginning of measurement in 2020 because this allows to do an evaluation of every change in tariff methodology (since 2020).

2. Rights and Obligations of the Parties

2.1. The Provider must ensure that the personal data of the data subject/s are obtained in a valid manner and that it has a legitimate legal ground and purpose for processing them. The Recipiënt will not check the validity of the legal ground and purpose and therefore cannot be held liable for any fraudulent acts committed by the Provider.

2.2. The Provider confirms that it has originaliy collected the personal data in context of its tasks carried out in the public interest pursuant to the 'Energiedecreet en -besluit' relating to management of the distribution network, such as maintenance, repair and improvement of the distribution network, as well as granting access to the network, management of meters, payment of premiums to promote the rational use of energy, reading of meters and counters at the access points of the distribution network and management of the metering data related to these access points. Processing by the Recipiënt involves further processing of personal data for purposes other than those for which the personal data was initially collected by the Provider. In accordance with the GDPR, such further processing may only be authorised if the processing is compatible with the purposes for which the personal data were initially collected.

The purpose for further processing in this case is scientific research by the Recipiënt. These processing activiti es are subject to an exception under Article 5(1)(b) GDPR and are, by consequence, not considered incompatible with the original purposes and do not require a separate legal basis.

2.3. The data made available will be retained by the Recipiënt for five years. This retention period can be justified in view of the time it may take to publish the results in a peer-reviewed scientific journal.

2.4. Personal data will not be processed with regard to passing on personal data to a third country or an international organisation, unless Recipiënt is obliged to conduct such processing by virtue of a provision of EU or Member State law to which Recipiënt is subject: in such case, Recipiënt will inform the Provider of this legal obligation prior to processing, unless legislation forbids such notification for urgent reasons of public interest.

2.5. Recipiënt will permit and facilitate audits, including inspections by the Provider or an auditor authorised by the Provider. More specifically, the auditor may access the premises and rooms of Recipiënt where the personal data is processed. The auditor must inform Recipiënt of this in a suitable manner and present themselves discretely at Recipient's premises and rooms within regular working hours. The costs of audits requested by the Provider will be borne by the Provider.

3. Technical and organisational measures

3.1. The personal data will be made available by Fluvius through the MSafe platform (https://filetransfer.fluvius.be/). Only limited recipients at UGent will be granted access via a link sent through e-mail, login and SMS verification are necessary to access the data. Shared files will be retained on the MSafe platform for a maximum of 30 days.

3.2. UGent's general data protection policy sets out the basic security level at the generic level. UGent's policy on "Working safely with personal data and confidential information", the Regulation on the correct use of the ICT infrastructure and UGent's Generic Code of Conduct provide general guarantees concerning:

- The protection of personal data against unauthorised access or viewing by third parties (confidentiality)
- The protection of personal data against unauthorised changes (integrity)
- The protection of personal data against destruction, loss or if for any reason, it is impossible to consult the data or there is a physical or technical incident, that availability of and access to the personal data will be reinstated in good time (availability)
- The right of data subjects to view their personal data (transparency).

3.3. Recipiënt will take all technical and organisational measures to guarantee a level of security that is in line with the risk relating to the storage and processing of personal data. This will take into account the state

of technology, the implementation costs, the nature, scope, context and processing objectives and the likelihood and seriousness of the various risks. Upon the Provider's request, Recipiënt will submit documentation describing the measures that have been taken.

3.4. Recipiënt shall implement at least the following organisational and technical security measures to protect the personal data received during further processing:

	yes	no	Clarification/motivation answer
1. Does your organisation have a written information security policy and -plan, which also includes the protection of personal data?	KI	☐	Yes, see https://helpdesk.ugent.be/security/tom.php and https://www.ugent.be/nl/univgent/privacy/gedragscode-persoonsgegevens.htm
2. Did you evaluate the risks and security needs specific to your organisation involving the processing of personal data?	KI	☐	Ghent University periodically carries out risk analyses of the security measures taken and carries out checks regarding compliance with the various information security procedures.
3. Have you identified the various carriers within your organisation involving personal data?	KI	☐	https://www.ugent.be/en/research/datamanagement/during-research/storage.htm lists the various carriers used at UGent. The data of this project will be stored on a network drive of Ghent University.
4. Are the internal and external staff involved in processing of personal data well aware of the confidentiality and security obligations regarding this data, arising from applicable legal requirements as well as from the information security plan?	KI	☐	See https://www.ugent.be/nl/univgent/privacy/gedragscode-persoonsgegevens.htm (a.o. section 5.1 2°). "All users are obliged to treat the personal data and/or confidential information to which they have access in a confidential manner."All people on the list of processors processing the communicated data will be made aware of the confidentiality and security obligations before gaining access to the data.

5. How is the confidentiality obligation of employees of the Recipiënt regulated (legal, statutory or contractual obligation)?	KI	☐	Section 5.12° of https://www.ugent.be/nl/univgent/privacy/gedragscode-persoonsgegevens.htm States that "AH users are obliged to treat the personal data and/or confidential Information to which they have access in a confidential manner."
6. Have you taken measures to prevent unauthorised or unnecessary physical access to carriers/systems containing personal data?	KI	☐	Section 5 https://helpdesk.ugent.be/security/tom-nl.pdf lists the measures to ensure the physical security of the UGent data centers.
7. Have you taken measures to prevent any physical damage that could compromise personal data?	KI	☐	Section 5 https://helpdesk.ugent.be/security/tom-nl.pdf lists the measures to ensure the physical security of the UGent data centers.
8. Have you taken measures to protect the various networks to which the equipment processing personal data is connected?	KI	☐	The internal network of Ghent University (UGentNet) is highly compartmentalized and equipped with advanced control mechanisms (firewall, intrusion detection & prevention) that adequately protect the internal network against unauthorized access and unwanted external actions. For this, there is also cooperation with Belnet, the Internet Service Provider for Ghent University. Up-to-date encryption protocols are used for the wireless networks to provide maximum protection for the transferred data. (Section 6 of https://helpdesk.ugent.be/security/tom-nl.pdf)
9. Do you have an up-to-date list of the authorised persons who have access to personal data and their respective level of access (creation, consultation, modification, destruction)?	KI	☐	UGent has installed an access authorisation mechanisms on its Information systems, see https://helpdesk.ugent.be/security/tom-nl.pdf (i.a. section 3.2)

10. Have you instalied an access authorisation mechanism on your Information systems so that personal data and the processing activities relating to it can only be accessed by the persons and applications expressly authorised to do so?	KI	☐	UGent has installed an access authorisation mechanisms on its Information systems, see https://helpdesk.ugent.be/security/tom-nl.pdf (i.a. section 3.2)
11. Is your Information system designed to permanently record the identity of those who have accessed personal data ?	KI	☐	The ICT infrastructure of Ghent University is checked by ICT system administrators with logging and monitoring, in order to ensure its proper functioning and to detect and prevent abuse. The level of detail is no more and the retention period no longer than necessary to achieve this goal. Depending on the type of data or Information and its degree of confidentiality, the logging is less or more detailed. For critical Information systems, accesses and actions are extensively logged. Data from this logging is confidential and will only be released after a formal request accepted by the board (eg a court order), (section 7.4 of https://helpdesk.ugent.be/security/tom-nl.pdf)
12. Have you provided for evaluation of the validity and effectiveness over time of the organisational and technical measures put in place to guarantee the security of personal data?	KI	☐	Ghent University periodically carries out risk analyses of the security measures taken and carries out checks regarding compliance with the various information security procedures. For general risk management in the field of data protection and IT security, the Internal Audit Department of Ghent University organizes selective audits. Results of such audits are communicated to the audit committee of Ghent University and to the Board of Directors of Ghent University (sectie 2.5 of https://helpdesk.ugent.be/security/tom-nl.pdf)
13. Have you provided for emergency procedures and reporting procedures in the event of security incidents involving personal data?	KI	☐	See section 11 of https://helpdesk.ugent.be/security/tom-nl.pdf.

14. Do you have updated documentation on the measures taken to protect personal data and the various processing activities involved?	E3	□	See https://helpdesk.ugent.be/security/tom-nl.pdf for UGent documentation on the measures taken to protect (personal) data.

3.5. In view of the risks accompanying the specific processing and nature of the data that must be protected, Recipiënt will take satisfactory additional safety measures that comply with relevant standards and quality requirements.

4. Article 5: Assistance to the Controller

4.1. Parties will provide each other with all Information and assistance that is necessary and/or may reasonably be expected to enable them respectively to fulfil their obligations under the GDPR.

4.2. The Recipiënt will act in accordance with the instructions issued by the Provider with respect to requests from data subjects with regard to their personal data. If a Data Subject submits a request concerning his or her personal data to the Recipiënt, such request will be immediately referred to the Provider.

4.3. Taking the nature of the processing into account and insofar as possible, Recipiënt will assist the Provider in fulfilling its obligation to comply with requests from data subjects to exercise their established rights by taking fitting technological and organisational measures.

5. Transfer

5.1. Personal Data may only be processed outside the European Economie Area or by an international organisation if the Recipiënt has informed the Provider beforehand in writing and in conformity with the GDPR.

5.2. Any request for transfer or provision of personal data to a third country, based on a court ruling or a decision by an administrative authority may only be complied with if the court ruling or decision is based on an international agreement, such as a treaty on mutual legal assistance between the third country submitting the request and the Union or a Member State. If this situation should arise, the Recipiënt will inform the Provider of the request immediately and prior to passing on the data.

6. Notification of a breach

6.1. The Recipiënt must immediately notify the Provider of every data leak they become aware of within the framework of the present collaboration in order to discuss the subsequent actions to be undertaken. All this must be agreed within the framework of the parties' respective obligations to notify the supervisory authority. Not only must Recipiënt notify the Provider of any data leaks, but the Provider must also inform the supervisory authority thereof as quickly as possible.

6.2. Recipiënt must notify the Provider of a data leak within **24 hours** its discovery, and if possible, inform the Provider of any steps they have already undertaken. Recipiënt does not have an obligation to notify the supervisory authority.

6.3. If it is likely that the breach concerning personal data presents a risk to the rights and freedoms of natural persons, the Provider will, in turn, inform the supervisory authority of a data leak within 72 hours of its notification of discovery, and if possible, inform the supervisory authority of any steps that have already been undertaken. If sensitive data is involved, the Data Subject must also be informed.

6.4. The notification referred to in clause 6.1 will in any case contain the following description or Information:

a) the nature of the data leak, if possible stating the categories of Data Subjects and registrations of personal data in question and, if they are to be approached, the number of Data Subjects and

registers of personal data in question;

b) the name and contact details of the data protection officer or another contact person who can supply more information if these persons are available;

c) the probable consequences of the data leak insofar as they can be overseen by the Recipiënt;

d) the measures proposed by Recipiënt to tackle the data leak, including if applicable, measures to limit any harmful consequences that may arise from it.

7. Processing by third parties

7.1. Recipiënt will not employ any third-party data processor without first obtaining permission to do so from the Provider and always in compliance with the relevant laws and regulations on the protection of personal data

7.2. If the Recipiënt employs a third-party data processor to perform specific processing activities on account of the Recipiënt, this third-party data processor will be bound through an agreement or other legal act pursuant to EU legislation or the laws of a Member State by the same obligations concerning data protection as those set out in this Agreement or other legal transaction between the Provider and Recipiënt, namely the obligation to provide sufficiënt guarantees with regard to the application of suitable technical and organisational measures to ensure that the processing is in compliance with prevailing legislation.

7.3. Recipiënt will, at the request of the Provider, provide an overview of the data processors processing the communicated data, and update this overview as necessary.

8. Liability

8.1. Unless explicitly agreed upon to the contrary, Recipient's obligations under this Agreement are on a best effort basis. Without prejudice to deviating mandatory legal provisions, Recipiënt is only liable for damage caused by non-compliance with these obligations if and insofar as this damage was caused by an intentional act, gross negligence or fraud. Recipiënt is not liable for any other errors.

8.2. The liability of either party to the other for any breach of this Agreement, any negligence or arising in any other way, whether direct or indirect, out of the subject matter of this Agreement, the Project and the Results, will not extend to any indirect damages or losses, or to any loss of profits, loss of revenue, loss of data, loss of contracts or opportunity even if the party bringing the claim has advised the other of the possibility of those losses, or if they were within the other party's contemplation.

=== END OF ADDENDUM ===