These Specific Terms "Personal Data" ("**Data Protection Agreement**" or "**DPA**") is intended ensuring compliance with Article 28 (3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("**GDPR**").

SUEZ has appointed a Personal Data Protection Officer, who can be contacted at privacy@suez.com.

1. DEFINITIONS

Unless otherwise defined in this DPA, capitalized terms shall have the meanings set forth in the Main Agreement. Terms beginning with a capital letter, used in the singular or plural, shall have the meaning given to them below:

Personal Data Regulation: means the GDPR including in particular any updated, additional, amended or other replacement provisions, guidelines, recommendations or regulations in force at the effective date of the Agreement and any national implementing or equivalent law, as well as any other law relating to privacy, security or protection of personal data, as applicable in all relevant jurisdictions.

The terms and expressions "**Personal Data**", "**Processing**", "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Data Breach**" and "**Supervisory Authority**" shall have the meaning given to them in the GDPR.

Partner Personal Data: means the Personal Data provided or made accessible by the Partner and processed by SUEZ for the provision of the Services.

Sub-Processor: means Data Processor hired by SUEZ to carry out specific Processing activities on behalf of the Partner.

2. SUEZ'S OBLIGATIONS AS A DATA PROCESSOR

2.1 Description of Processing

Details of the Processing, and in particular the categories of Personal Data and the purposes for which the Partner's Personal Data is processed, are set out in Annex 1-1 of the DPA.

2.2 Instructions

SUEZ Processes the Partner's Personal Data as a Data Processor, solely in accordance with the instructions and for the purposes documented in Annex 1-1 of the DPA by the Partner as the Data Controller, unless SUEZ is required to do so under European Union law or the law of the Member State to which it is subject. In this case, SUEZ informs the Partner of this legal obligation prior to the Processing, unless it is prohibited from doing so by law for important reasons of public interest. If SUEZ considers that an instruction from the Partner constitutes a breach of the Regulation on personal data, it agrees to inform the Partner.

2.3 Processing security

SUEZ implements the appropriate technical and organisational measures to ensure the security of the Partner's Personal Data and in particular to prevent any Data Breach. The measures implemented by SUEZ are specified in Annex 1-2 of the DPA.

SUEZ ensures that the persons authorised to process the Partner's Personal Data agree to respect confidentiality or are subject to an appropriate legal obligation of confidentiality.

2.4 Sub-Processors

SUEZ is authorised to use Sub-Processors listed in Annex 1-3 of the DPA.
SUEZ informs the Partner of any addition or replacement of Sub-Processors. The Partner may object to the recruitment of a Sub-Processor within fifteen (15) days of receipt of the information, for reasons relating to the Regulations on personal data, without affecting SUEZ's right to use the new Sub-Processor(s) after the notice period indicated above.
In the event of an objection by the Partner, the Parties agree to discuss in good faith how to resolve the objection. SUEZ may then decide to:

- take reasonable measures to meet the Partner's objection by using the services of the Sub-Processor;
- not use the Sub-Processor; or
- use the Sub-Processor.

SUEZ notifies the Partner of its decision without delay. Within a period of fifteen (15) days upon receipt of the notification from SUEZ, if the Partner maintains its objection for reasons relating to the Regulations on personal data, SUEZ may terminate the service using the new Sub-Processor in compliance with the termination conditions set out in the Agreement. The Partner agrees the use of the proposed Sub-Processor until the effective date of termination.
When a rapid replacement is required for reasons of security or urgency, a Sub-Processor may be replaced without notice by SUEZ. SUEZ informs the Partner of the replacement of the Sub-Processor as soon as possible after its appointment.
When SUEZ recruits a Sub-Processor to carry out specific processing activities on behalf of the Partner, it does so by means of a contract which imposes on the Sub-Processor, in substance, the same personal data protection obligations as those imposed on SUEZ under this DPA. SUEZ shall ensure that the Sub-Processor complies with the obligations to which it is itself subject under this DPA and the Personal Data Regulations.

2.5 International Transfers

SUEZ only transfers Personal Data of the Partner outside the European Union on the basis of documented instructions from the Partner or in order to comply with a specific legal or regulatory obligation to which SUEZ is subject. If SUEZ or one of the Sub-Processors transfers Personal Data of the Partner outside the European Union as described in Annexes 1-2 and 1-3, SUEZ agrees to comply with the requirements of Chapter V of the GDPR.

3. ASSISTANCE TO THE PARTNER - DATA CONTROLLER

3.1 Responses to requests from data subjects to exercise their rights

When SUEZ receives a request from a Data Subject to exercise his/her rights, SUEZ informs the Partner of this request without delay. SUEZ does not itself follow up this request, unless otherwise instructed by the Partner. SUEZ assists the Partner in fulfilling its obligation to respond to requests from Data Subjects to exercise their rights.

3.2 Compliance with the Partner's obligations

SUEZ helps the Partner to ensure compliance with the following obligations, considering the nature of the Processing and the information available to SUEZ:

- the obligation to carry out a data protection impact assessment where this is required within the limit of one working day of service;
- the obligation to consult the competent Supervisory Authority where this is required as a result of the data protection impact assessment;
- the obligation to ensure that the Partner's Personal Data is accurate and up to date, by informing the Partner without delay if SUEZ learns that the Partner's Personal Data that it processes is inaccurate or has become obsolete;
- the obligations set out in Article 32 *et seq* of the RGPD.

4. NOTIFICATION OF DATA BREACHES

In the event of a breach related to data processed by SUEZ on behalf of the Partner, SUEZ shall inform the Partner as soon as possible after becoming aware of it. This notification shall contain:

- a description of the nature of the Data Breach;
- details of a contact from which further information can be obtained about the Data Breach;
- its likely consequences and the measures taken or proposed to be taken to remedy the Breach, including mitigation of any adverse consequences.

Where it is not possible to provide all the information at the same time, the initial notification will contain the information available at that time and, as it becomes available, additional information will be provided as soon as possible thereafter.

5. INFORMATION AND AUDIT

SUEZ shall make available to the Partner, upon its request, all information necessary to demonstrate compliance with the obligations set out in the DPA, including any audit or certification report such as SOC, ISO, NIST, PCI DSS, HIPAA or any other equivalent document issued by a qualified third-party auditor or certifier within the last twelve (12) months.

If the Partner considers that the information provided by SUEZ is insufficient to demonstrate compliance with the obligations set out in the DPA, the Partner shall inform SUEZ in writing, specifying the reasons why the information provided is insufficient. SUEZ then provides the Partner with the relevant additional information.

If the Partner considers the additional information provided by SUEZ to be insufficient, the Partner may carry out or have carried out an audit of the Processing covered by the DPA, up to a limit of once a year, except in the event of a Data Breach related to data processed by SUEZ.

The Partner informs SUEZ in writing of its intention to carry out an audit, complying with twenty (20) working days' notice, except in the case of a shorter period in the event of a Data Breach related to data processed by SUEZ. The timing and scope of any audit shall be agreed between the Parties acting reasonably and in good faith. The Partner shall bear the costs of any audit initiated.

The Partner appoints the third-party auditor, non-competitor of SUEZ, subject to the written and specific agreement of SUEZ.

6. SUSPENSION AND TERMINATION

6.1 Suspension and Termination by the Partner

In the event of SUEZ failing to fulfil its obligations under the DPA, the Partner may instruct SUEZ to suspend Processing until the latter has complied with the DPA.

The Partner is entitled to terminate the Agreement in accordance with the termination conditions set out in the Agreement if:

- Processing by SUEZ has been suspended by the Partner pursuant to this article 6.1 and compliance with the DPA has not been restored within one month of the suspension;
- SUEZ is in serious or persistent breach of this DPA or its obligations under the Personal Data Regulations;
- SUEZ does not comply with a binding decision of a competent court or the competent Supervisory Authority concerning its obligations under the DPA or the Personal Data Regulations.

6.2 Termination by SUEZ

SUEZ is entitled to terminate the Agreement in accordance with the termination conditions set out in the Agreement, if after informing the Partner that its instructions infringe the Personal Data Regulations, the Partner maintains its instructions in the same terms.

7. DATA RETURN AND DESTRUCTION

On expiry or after termination of the Agreement or upon request of the Partner, SUEZ agrees to destroy or return to the Partner, at the latter's choice, within the period agreed between the Parties, all the Partner's Personal Data, including any copies that may have been made on any medium whatsoever, except in the event of the need for retention required by applicable law.

***

ANNEX 1-1 – PROCESSING DESCRIPTION

Purpose of Processing	Type of Processing	Categories of data processed	Categories of data subject	Place of processing	Duration of processing	Data retention period	Sub-Processor
Provision of the ON'connect™ metering Service: - Monitoring of consumption - Monitoring of meter metrology (transmitter battery alert, monitoring of meter/transmitter associations, asset upgrade maintenance) - Alert management (leak alerts, over-consumption alerts)	Collection, storage, recording, making available, archiving	**Personal data:** current consumption index, daily consumption index, night-time volume, return water index, etc. **Remote reading data**: Remote reading index (15m, 1h, 6h, 24h), midnight interpolated index, information on minimum and maximum flow rates, maximum instantaneous flow rate, leak volume, alarms from transmitters (freezing, battery, fixing, access, overflow, backflow, water leak, risk of blocked meter) **Location data**: GPS coordinates of the service point	Subscribers to water distribution contracts	France	Duration of the Contract	**Personal data**: 5 years **Remote reading data**: 5 years **Location data**: equipment lifetime **Point-of-service characteristics**: equipment lifetime	**Cloud temple** (hosting) **Accenture** (Third-party application maintenance)

		Service point characteristics: service point ID, service point postal address, INSEE code, meter diameter, meter number, transmitter number, meter pulse weight, transmitter battery level, transmitter temperature, etc.						

Provision of the ON'connect™ coach Service: Customer consumption monitoring and consumption advice	Collection, storage, recording, making available, archiving	**Personal data**: current consumption index, daily consumption index, night-time volume, return water index, etc. **Remote reading data**: remote-read indexes (15m, 1h, 6h, 24h), midnight interpolated index, information on minimum and maximum flow rates, maximum instantaneous flow rate, leak volume, alarms from transmitters (freezing, battery, fixing, access, overflow, backflow, water leak, risk of blocked meter) **Location data**: GPS coordinates of the service point **Service point characteristics**: service point ID, service point postal address, INSEE code, meter diameter, meter number,	Subscribers to water distribution contracts	France, Ireland	Duration of the Contract	**Personal data:** 5 years **Remote reading data**: 5 years **Location data**: equipment lifetime **Point-of-service characteristics**: equipment lifetime	**Cloud temple** (hosting) **Microsoft Azure** (hosting)	

		transmitter number, meter pulse weight, transmitter battery level, transmitter temperature, etc.						

Provision of the Opti'Revenue service : Management of water meters (monitoring of technical condition and analysis of consumption)	Collection, storage, recording, making available, archiving	**Meter data**: daily meter readings, daily meter alarms, daily transmitter alarms **Customer data**: contact details / postal address, customer identification, customer number and point of service number **Financial data**: meter replacement and installation costs	Subscribers to water distribution contracts	Spain	Duration of the Contract	**Daily data**: 2 years. **Monthly data**: 5 years	**Siemens** (Saas provider for water meters management)	

ANNEX 1-2 - Description of technical and organisational security measures

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES			SERVICES		
			ON'connect ™ metering	ON'connect ™ coach	Opti' Revenue
1	**Managing data security**	Making security an issue shared and supported by the management team	X	X	X
		Provide an information security policy and thematic security policies	X	X	X
		Provide an information security organisation in which functions and responsibilities are defined	X	X	X
		Provide a policy for classifying and marking data	X	X	X
		Provide a personal data protection policy	X	X	X
		Identify the processing of personal data (register)	X	-	X
		Regularly assess the effectiveness of the security measures implemented and adopt a continuous improvement approach	X	X	X
2	**Defining a framework for users**	Draw up an IT charter setting out the terms and conditions for using IT systems, security rules and the administrative resources in place	X	X	X
		Make the Charter binding and set out the penalties for non-compliance	-	-	-
3	**Involving and training users**	Raising the awareness of those handling data, particularly personal data	X	X	X
		Documenting operating procedures	X	X	X
4	**Authenticating users**	Provide a unique login for each user	X	X	X
		Adopt the SUEZ password policy	X	X	X
		Force the user to change the password assigned automatically or by an administrator	X	X	X
5	**Managing authorisations**	Define authorisation profiles	X	X	X
		Validate all requests for authorisation	X	X	X
		Delete users' access permissions as soon as they are no longer authorised to access a room or resource, and at the end of their contract.	X	X	X

		Carry out an annual review of authorisations	X	X	X
6	**Securing workstations**	Provide an automatic session locking procedure	-	-	X
		Installing and configuring an Internet filtering proxy	X	X	X
		Use regularly updated antivirus software	X	X	X
		Deploy security updates as soon as possible	X	X	X
		Limit user rights to the strict minimum according to their needs	X	X	X
		Encourage the storage of user data on a regularly backed-up space accessible via the internal network	X	X	X
		Securely erase data on a workstation before it is reassigned	X	X	X
		Obtain the user's agreement before any work is carried out on their workstation	X	X	X
7	**Securing mobile computing**	Raising users awareness of the specific risks of being on the move	X	X	X
		Provide means of encrypting mobile equipment	X	X	X
		Requiring a secret for unlocking smartphones	X	X	X
8	**Protecting the IT network**	Limit network flows to what is strictly necessary	X	X	X
		Securing Wi-Fi networks, in particular by implementing the WPA3 protocol	X	X	X
		Securing remote access to mobile computing devices via VPN	X	X	X
		Partitioning the network, for example by setting up a DMZ (demilitarised zone)	X	X	X
9	**Securing servers**	Restrict access to administration tools and interfaces to authorised personnel only	X	X	X
		Install critical updates without delay, after testing them where necessary	X	X	X
		Use malware detection and removal software	X	X	X
		Carry out back-ups and regularly check their integrity and ability to restore them	X	X	X
		Set up an event logging system	X	X	X
10	**Securing websites**	Securing data exchange flows by obtaining appropriate certificates and the mandatory use of TLS	X	X	X
		Limit communication ports to those strictly necessary for the correct operation of the application	X	X	X

		Restrict access to administration tools and interfaces to authorised personnel only	X	X	X
		If cookies are used that are not necessary for the service, the user's consent must be obtained.	X	X	X
		Check that no secrets or personal data pass through URLs	X	X	X
		Limit the information returned when creating a user account or resetting a password	X	X	X
		Adopting best practice in IT development (OWASP Top 10, etc.)	X	X	X
11	**Manage IT developments**	Integrate data protection, including its requirements in terms of personal data security, right from the design stage	X	X	X
		Use secure components and tools recognised by the community	X	X	X
		Implement measures against common attacks on databases (SQL code injection, etc.)	X	X	X
		For any development aimed at the general public, consider the parameters that influence respect for privacy.	X	X	X
		Avoid using free text or comment areas	-	-	-
		Carry out comprehensive tests before releasing or updating a product	X	-	X
		Carry out IT development and testing in a separate IT environment from production	X	X	X
		Ensuring that no secrets (authentication or encryption) are used when submitting code to a version management tool	X	X	X
		Use fictitious or anonymised data for development and tests	X	X	X
		Carry out a non-regression test and/or a code review before any update goes into production	-	-	X
12	**Protecting premises**	Restrict access to premises	X	X	X
		Install intruder alarms and check them regularly	X	X	X
		Install smoke detectors and fire-fighting equipment and inspect them annually	X	X	X
		Establish rules and means of controlling visitor access, at least by having visitors escorted out of the public reception areas	X	X	X
		Physically protect IT equipment by specific means	X	X	X
13		Encrypting data before it is recorded on a physical medium for transmission to a third party	X	X	X

	Securing external exchanges	When sending via a network: encrypt sensitive documents to be transmitted, use a secure protocol (SFTP, HTTPS, etc.) and ensure the confidentiality of secrets.	X	X	X
		Transmit the secret in a separate transmission via a different channel	X	X	X
		Open an external file only if the sender is known and after it has been subjected to an antivirus scan	X	X	X
14	**Managing subcontracting**	Only use subcontractors with sufficient guarantees	X	X	X
		Include specific safety clauses in subcontractor contracts	X	X	X
		Ensuring that the guarantees provided are effective (e.g. safety audits, PAS, visits)	X	X	
15	**Managing the maintenance and end-of-life of hardware and software**	Include security clauses in maintenance contracts with service providers to govern their access to information systems	X	X	X
		Supervision of third-party interventions by an organisation manager	X	X	X
		Securely delete data from equipment before it is scrapped, sent to a third party for repair or at the end of a rental contract	X	X	X
16	**Tracing operations**	Provide a logging system	X	X	X
		Inform users about the introduction of the logging system	X	X	X
		Protecting logging equipment and logged information	-	-	X
		Actively analyse the traces collected, in real time or in the short term, to detect the occurrence of an incident	X	X	X
17	**Save**	Make frequent data back-ups	X	X	X
		Store at least one backup on a site that is geographically separate from the operating site	X	X	X
		Protecting back-ups, both during storage and transportation	X	X	X
		Regularly test the restoration and integrity of back-ups	X	X	X
18	**Planning for business continuity and recovery**	Draw up an IT business continuity plan (BCP) and recovery plan (DRP)	-	-	X
		Ensure that users, service providers and subcontractors know who to alert in the event of an incident	-	-	X
		Carry out regular exercises to apply the business continuity or recovery plan	X	X	X
19		Regularly analyse the traces collected and process alerts raised by the logging system	-	-	X

	Managing incidents and breaches	Establish a procedure(s) detailing the incident management process, including the management of data breaches, and define the criteria for qualifying a breach	X	X	X
		Assess the risk to individuals caused by the violation	X	X	X
		Keep an internal register of all personal data breaches	X	X	X
		Notify the CNIL, within 72 hours (as provided for by the RGPD), of breaches presenting a risk to the rights and freedoms of individuals and inform the data subject	X	X	X
20	**Risk analysis**	Carry out a risk analysis, even a minimal one, on the data processing envisaged	X	X	X
		Identify the personal data processing operations for which a data protection impact assessment (DPIA) is mandatory under the RGPD	X	X	X
		Monitor the progress of the action plan decided on following the risk analysis.	X	X	X
21	**Encryption, hashing, signing**	Use recognised and secure algorithms, software and libraries	X	X	X
		Use appropriate key sizes	X	X	X
		Keep secrets and cryptographic keys securely	X	X	X
22	**Cloud: Cloud computing**	Mapping data and processing in the Cloud	X	X	X
		Including Cloud services in risk analysis	X	X	X
		Configure any security tools provided by the supplier	X	X	X
		Ensure the same level of security in the cloud as on site	X	X	X
23	**Mobile applications: Design and development**	Consider the specificities of the mobile environment to reduce the personal data collected and limit the permissions required (including authentication)	X	X	X
		Secure communications (TLS) and store cryptographic secrets using packaging	X	-	X
		Consider the possibility of the operating system automatically backing up personal data	X	-	X
		Use an authentication method that corresponds to the desired level of security	X	-	X
24	**Artificial intelligence: design and learning**	Implement a development team with multidisciplinary skills, ensure it is trained in good security practices and raise awareness of the vulnerabilities specific to AI.	X	-	X
		Implement a mandatory procedure for continuous development and integration, in particular for changes to production code	X	X	X
		Check the quality of data and annotations, the presence of bias and the reliability of data sources	X	X	X
		Avoid partial or total copying of databases and use fictitious or summary data.	X	X	X

		Document system operation and limitations	-	-	X
		Check the legitimacy of system users when the system is made available as a service	X	X	X
		Provide a system audit plan covering software, hardware and organisational measures such as procedures for human supervision of the AI system.	X	X	-
25	**API: Application Programming Interface**	Organise and document the security of access to APIs and data	-	-	X
		Limit data sharing to the people and purposes intended	X	X	X

ANNEX 1-3 - List of Sub-Processors

Sub-Processor acting on behalf of the Service Provider Company name Postal address, country E-mail address of a representative and the DPO	**Countries in which processing is carried out**	**Description of outsourced processing**	**Adequacy tools used in the event of Data transfers (and additional technical and organisational security measures, where applicable)**
Cloud Temple Le Belvédère, 1-7 Cr Valmy, 92800 Puteaux - SPACES	France	Hosting	N/A
Accenture - 118, avenue de France, 75013 Paris **DPO**: dataprivacy@accenture.com	France, Mauritius, Vietnam	Third-party application maintenance (ON'connect™ metering service)	Standard contractual clauses
Microsoft Ireland Operations Limited - One Microsoft Place, South Country Business Park, Leopardstown, Dubin 18, D18 P521 - Ireland **Microsoft France SAS** - 39 quai du Président Roosevelt, Issy les Moulineaux, 92130, France **DPO**: Microsoft EU Data Protection Officer in Ireland, +353 (1) 706-3117	Ireland, United States	Hosting	Adequacy decision (Data privacy framework)

Siemens Industry Software SAS - 107 Avenue de la République, 92320 Hauts-de-Seine, France **Siemens Industry Software, S.L.U. -** Tres Cantos - Madrid (Spain) - Ronda de Europa 5, 28760 Tres Cantos, Madrid, Spain **DPO**: dataprivacy@siemens.com	Spain, Germany	Supply of a Saas-based solution for managing water meters	N/A