Framework Agreement for access and use of the SL-ATR system

Party of the first part, **ENAGÁS GTS, S.A.U.** (hereinafter, "ENAGAS GTS")

And party of the second part, **SUBJECT OF THE GAS SYSTEM** (hereinafter, "SUBJECT")

For the purposes of this Agreement, ENAGAS GTS and SUBJECT shall be jointly referred to as the "Parties" and individually and indiscriminately as the "Party".

Both parties recognise sufficient legal capacity to execute this Agreement.

RECITALS

1. Whereas ENAGAS GTS, in its status as the Technical Manager of the Gas System, has developed:

    a. the information system SL-ATR - Third-party Access Logistics System - in accordance with the Detailed Protocol PD-04 "Communication Mechanisms".

    b. the platform that makes it possible for exchanges of gas between agents of the Spanish Gas System.

    Hereinafter, the term "SL-ATR system" must be understood as including both the SL-ATR information system as well as the MS-ATR platform.

2. Whereas SUBJECT, as Agent of the Gas System, is interested in having access and being a user in the SL-ATR system.

3. Whereas both Parties agree to execute this Agreement for access and use of the SL-ATR system, in accordance with the following

CLAUSES

1. Scope of Agreement

The purpose of this Agreement is for ENAGAS GTS to provide SUBJECT with the services of access, in terms of security, and use of the SL-ATR system and the MS-ATR platform, with the rights and obligations defined in this Agreement.

2. Publication of the Agreement. Document of Accession

This Agreement shall be published on the Enagás corporate website and digitally signed by Enagás GTS for the purpose of electronically setting the publication date and guaranteeing the integrity of its content in any downloaded electronic copy. Any amendments to the text of the Agreement shall be duly reported to SUBJECT and included in the new version of the Agreement, which shall replace the previous one and shall be published as described above.

The Agreement shall be signed by ENAGÁS GTS and SUBJECT through the electronic signing of the Document of Accession to the same.

3. Service conditions

3.1 Through the SL-ATR Portal, SUBJECT, as Gas System Agent, shall have an exclusive channel of communication for publication of information and contents to these users, with this being the sole point of access and interaction for users with the SL-ATR system.

3.2 Through the SL-ATR system, SUBJECT, as Gas System Agent, shall have the communication tool that provides support to management of the complete gas cycle; request for capacity, contracting, programming and nominations, measurements, distribution, balances and billing. All this management shall be in accordance, in terms of periods and methods, with the System Technical Management Regulations (NGTS) and their Detailed Protocols (PD).

3.3 ENAGAS GTS shall keep the systems updated, and the system shall be easily accessible and guarantee that the information supplied is

up-to-date, as well as its security and confidentiality, and with regard to the principles of transparency, objectiveness and non-discrimination.

3.4 The SUBJECT must be equipped with the Hardware and Software means required to access the systems. The detail of these means are shown on the ENAGAS website. The twin-factor mechanism of access to the SL ATR is carried out via the web from the computer or mobile device, with the person identifying themselves using the corporate email address and their mobile telephone number, the latter previously registered and associated to the user in the authentication system of Enagás S.A.

3.5 Authorisation for the exchange of information through XML messages with the SL-ATR system requires a Technical Accreditation to be obtained, the details of which are shown in clause 4 below.

4. Technical Accreditation

The exchange of information shall be carried out in some cases by entering data and on-screen and other times using one of the following integration methods:

- attaching XML files by screen
- Sending information by invoking web services

The use of these two mechanisms requires a prior technical accreditation stage.

The Technical Accreditation certifies that the agents can perform exchanges of information with the SL-ATR through the mechanisms provided by ENAGAS GTS:

- XML files via SL-ATR
- XML files via Web Services

This accreditation is associated to the exchanges of information of each process of the SL-ATR through XML files.

The application used to request Technical Accreditation is available on the SL-ATR Portal.

The Technical Accreditation of the SUBJECT is an essential condition to be able to operate with the new communication mechanisms of the SL-ATR. Accordingly, and until this has been obtained, there can be no complete access to the functionality to which this Agreement gives the right.

5. Rights and obligations of SUBJECT

5.1 SUBJECT shall be entitled to access the SL-ATR system under the same conditions as the other system users.

5.2 SUBJECT shall furnish ENAGAS GTS with the details concerning their company's user for which access is requested and/or modification of the profile and/or removal as a company staff member.

5.3 SUBJECT, in consideration for the services covered by this Agreement, shall pay ENAGAS GTS the price established in Clause 7.

5.4 SUBJECT shall collaborate with ENAGAS GTS and keep the latter informed of all aspects that may be necessary for better development of the services under this Agreement.

5.5 SUBJECT shall immediately notify ENAGAS GTS of any irregularity in the use of access codes or suspected unauthorised use of these, or in the event of having been disclosed to unauthorised persons.

5.6 SUBJECT shall be responsible for ensuring the integrity of its systems and software and, specifically, it shall introduce and impose the appropriate measures to protect its software systems against unauthorised access, as well as against download and effects of any virus.

5.7 SUBJECT must obtain the Technical Accreditation referred to in clause 4 of the Agreement for authorisation for the exchange of information through XML files.

6. Rights and obligations of ENAGAS GTS

6.1 ENAGAS GTS must have the technical means required for the proper performance of the SL-ATR system and the MS-ATR platform. ENAGAS GTS reserves the right to conduct the technical modifications it deems appropriate to improve the performance of these systems.

6.2 ENAGAS GTS may suspend any person from accessing the systems if this person is using them contrary to the conditions of this Agreement and/or in detriment to third parties, and/or is suspected of irregular conduct with regard to the aforementioned systems.

6.3 On request by SUBJECT, communicated in accordance with Clause 10 of this Agreement, ENAGAS GTS shall proceed to register in the SL-ATR system those persons detailed in Appendix I of the Document of Accession to this Agreement. Similarly, ENAGAS GTS shall proceed to

de-register those persons included in the aforementioned Appendix I that are notified in the same way by SUBJECT. The aforementioned modification shall be undertaken through an update of Appendix I. ENAGAS GTS shall introduce review mechanisms for users' activity and shall proceed to block those persons detailed in the aforementioned Appendix I that have not accessed the SL ATR system for a long time, following email notification to SUBJECT, in order to formalise the de-registration within a deadline of one month thereof.

7. Price

The services under this Agreement are provided free of charge. However, in the future ENAGAS GTS reserves the right to introduce a price for the aforementioned services on the basis of duly informed criteria.

8. Liabilities

8.1 Each Party shall answer to the other party for damages caused to the other as a consequence of acts or omissions involving gross negligence or deceit.

8.2 Liability for indirect and emerging damages is hereby excluded, for illustrative purposes including loss of earnings, loss of business.

8.3 The Parties hereby mutually exonerate each other from any damage that might occur, irrespective of the cause, in their respective facilities and/or systems, as well as their personnel and/or properties, except as provided for in subclause 8.1 above.

8.4 ENAGAS GTS informs SUBJECT that the supply of electronic services may be subject to different technical difficulties. These difficulties include, inter alia, malfunctions, delays, software and hardware performance problems, software or inadequate communications link or other causes. Such difficulties could lead to a potential economic loss and/or loss of data. The performance of businesses through any electronic system exposes SUBJECT to risks associated to the system, malfunctions of software and other components. In the event of malfunctions of the system, software or other components, SUBJECT may be unable to enter orders, perform transactions, modify or cancel orders for a certain period of time. The software system or the malfunctions of its components could lead to the loss of orders or the priority of such orders.

ENAGAS GTS refutes liability for any damage caused to the user as a consequence of the aforementioned technical problems.

8.5 ENAGAS GTS shall not be liable for direct damages incurred by SUBJECT or for indirect and/or consequential damages, loss of production, loss of earnings that may be caused to SUBJECT as a consequence of the normal or abnormal performance of the systems, irrespective of the reasons, unless there is gross negligence or deceit on the part of ENAGAS GTS.

8.6 ENAGAS GTS is not liable for the documentation of the bilateral operations between the counterparties or for the settlement of these.

8.7 ENAGAS GTS provides the tools for sending and the appropriate filter mechanisms so that SUBJECT can control the entry of data in the systems, whereby ENAGAS GTS shall not be liable for any errors entered by SUBJECT.

9. Confidentiality

ENAGAS GTS shall not disclose any confidential information related to use of the SL-ATR system and of the MS-ATR platform by SUBJECT, except:

a) When this is required through applicable regulations or an order from any competent administrative or judicial authority.

b) To the authorised employees of SUBJECT.

10. Communications

All communications between the Parties concerning this Agreement shall be made in accordance with the provisions set out in the Documents of Accession to the same.

11. Termination of the Agreement

This Agreement may be terminated on any of the following grounds:

11.1 At the discretion of the Party not in breach, whenever there is serious breach by the other Party of any of its main obligations under this

Agreement. To this end, the Party that considers there to be an event of breach shall notify the other Party of said breach, duly compelling them to rectify said breach. Failure to rectify the breach within 10 calendar days following the aforementioned notification shall entitle the Party not in breach to terminate this Agreement.

11.2 Through termination of the initial term or any of the extensions thereto, in accordance with the terms laid down in Clause 12.

11.3 Through the will of either Party, duly providing the other Party with at least two months' notice in a manner requiring acknowledgement of receipt.

11.4 At the discretion of either Party, when an event of force majeure may hinder or prevent compliance with the Agreement for more than one month.

11.5 If SUBJECT ceases its activity as a Gas System Agent.

11.6 Through breach of the obligations set out in paragraph two of Clause 13.

11.7 By mutual agreement of the parties,

12. Duration

This Agreement shall come into force from the day following the signing of the Document of Accession to the same and shall have an initial term of two years. It may be tacitly extended for successive periods of one year unless one Party notifies the other of its wish to terminate the Agreement two months before the Agreement termination date or the expiry of any of its extended periods.

13. Assignment

ENAGAS GTS may convey, on a singular basis and through any act in the law that provides for such transfer, its position in this Agreement to any company that forms part of the ENAGAS Groupand must notify this to SUBJECT.

SUBJECT cannot assign or transfer the rights and obligations stemming from this Agreement to third parties in full or in part without prior written consent from ENAGAS GTS. Breach of this obligation by SUBJECT shall be sufficient grounds for termination of this Agreement.

Under all circumstances, the assignee shall fully assume all rights and obligations arising under this Agreement, whether before or after the time the assignment is effective.

14. Applicable law and Jurisdiction.

This Contract shall be governed by common Spanish legislation.

The Parties hereby undertake to comply with this Agreement in good faith, using negotiations and amicable agreements to resolve any differences that may arise between them with regard to the application, development, compliance, interpretation and performance of the same.

The Parties expressly submit to the jurisdiction and terms of reference of the Courts of Madrid for ruling on any dispute or litigation concerning the Agreement, in particular with regard to its interpretation, performance or non-performance, whether before or after its expiry, and which in the opinion of one of the Parties they are unable to resolve through mutual agreement.

The submission of conflicts between the Parties to the foregoing judicial bodies does not entitle either Party to suspend compliance with their obligations under this Agreement.

15. PERSONAL DATA PROTECTION

15.1 Purpose

ENAGÁS GTS, as a consequence of the activity it provides to the DATA SUBJECT, accesses personal data that is the responsibility of the DATA SUBJECT. For these purposes, the DATA SUBJECT will be considered the data controller (hereinafter DATA CONTROLLER) and ENAGÁS GTS will be considered the data processor (hereinafter, DATA PROCESSOR) in accordance with the provisions of articles 28 and 29 of the (EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, GDPR).

15.2 Description of the Processing

The data affected by this Agreement will be used for the sole purpose of identifying and authenticating the persons who access the systems that are the subject of the Agreement on behalf of the DATA CONTROLLER.

15.3 Information affected

For the performance of the services arising from compliance with the purpose of the assignment, the DATA CONTROLLER places the following information at the disposal of the DATA PROCESSOR.

- Name and Surname(s).
- National Identity Document
- Work email address.
- Work mobile telephone number.

15.4 Obligations of the DATA CONTROLLER

The DATA CONTROLLER undertakes to:

1 Furnish the DATA PROCESSOR with the data covered by the processing specified in this Agreement.

2 Carry out an assessment of the risks involved in the processing and, when appropriate, an impact assessment of the data processing that the data processor must carry out.

3 Notify the competent Supervisory Authority of any security breaches in accordance with article 55 of the GDPR without undue delay, and in any case within the 72-hour deadline from becoming aware of these. If the supervisory authority is not notified within 72 hours, the reasons for the delay must be appended.

4 Notify the data subjects of any data security breaches as expeditiously as possible, when it is likely that the violation poses a high risk to the rights and freedoms of natural persons.

5 Ensure, prior to and throughout the processing, compliance with the GDPR by the DATA PROCESSOR.

6 The DATA CONTROLLER must facilitate the right to be informed at the time when the data is collected. The DATA PROCESSOR does not collect personal data for and on behalf of the DATA CONTROLLER. The data accessed by the DATA PROCESSOR pursuant to this Agreement must be obtained and processed pursuant to prevailing regulations governing personal data protection.

15.5 Obligations of the DATA PROCESSOR

Taking into account the nature, scope, context and purposes of the processing, the DATA PROCESSOR will apply the technical and organisational measures defined in this Agreement to guarantee a level of security appropriate to the involved risk, complying with the following obligations:

1 Principle of data minimisation

Access the personal data that is the responsibility of the DATA CONTROLLER only when it is essential for the proper performance of the services for which the party has been contracted.

2 Restriction of purpose

Not to assign, apply or use the personal data that are the responsibility of the DATA CONTROLLER for a purpose other than that

specified in this Agreement, or in any other way that implies a breach of the instructions of the DATA CONTROLLER.

3 Responsibility

To assume the status of DATA CONTROLLER if data are used for a purpose other than compliance with the purpose of the Agreement, disclosed or used in breach of the stipulations of the Agreement or the obligations of prevailing regulations, duly answering for any infringements incurred.

4 Non-disclosure of data

Not to permit access to personal data provided by the DATA CONTROLLER to any employee under their charge that does not need to access these data to provide the services contracted.

Not to reveal, transfer, assign or communicate in any other way the personal data that are the responsibility of the DATA CONTROLLER, either verbally or in writing, by electronic means, hard copy or through IT access, not even for safeguarding purposes, to any third party, unless there is prior authorisation or instruction from the DATA CONTROLLER.

5 Records of Processing Activities

If required to keep Records of Processing Activities under article 30 of the GDPR, the DATA PROCESSOR will keep a record of all categories of processing activities carried out on behalf of the DATA CONTROLLER, which contains the information required under article 30.2 of the GDPR.

6 Training

Guarantee the necessary training in terms of protection of personal data of the persons authorised to process personal data.

7 Enquiries to the Supervisory Authority

Support the DATA CONTROLLER in making preliminary enquiries to the Supervisory Authority, when applicable.

8 Supervision

Provide the DATA CONTROLLER with all of the information required to demonstrate compliance with its obligations, as well as to conduct the audits or inspections undertaken by the DATA CONTROLLER or another auditor authorised by this party.

9 Security measures

Adopt and apply the following security measures, in accordance with the assessment of the risk carried out and, where appropriate, the Impact Assessment, pursuant to article 32 of the GDPR (that guarantees the security of the personal data of the DATA CONTROLLER), to avoid their alteration, loss, processing or unauthorised access, in light of the state-of-the-art, the nature of the data stored and the risks to which they are exposed, whether as a consequence of human action or physical or natural means.

The security measures applicable to data processing are for the following purposes:

a) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

b) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

c) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, and;

d) the pseudonymisation and encryption of personal data, where necessary.

To this end, the following measures are introduced:

a) Control of access to the SL-ATR systems through the establishment of identification and authentication measures.

b) Policies, rules and procedures for the secure management of any type of medium that stores personal data and allows their transfer outside the main data processing locations.

c) Making periodic backup and retrieval copies.

d) Definition of the duties and obligations of each one of the users (employees) or profiles of users with access to data and the information systems.

e) Conducting training actions on the knowledge of these duties and the consequences of non-compliance.

f) Notification and recording of security incidents that may pose a risk to the confidentiality or integrity of the data as well as notification of breaches in the security of personal data in accordance with the established procedure.

10 Notification of data security breaches

The DATA PROCESSOR will notify the DATA CONTROLLER, without any undue delay, and in any case within the 72-hour deadline, of any security breaches of personal data under their charge of which they become aware, together with all relevant information for the documentation and reporting of the incident.

If available, at least the following information will be provided: (i) Description of the nature of the breach of personal data security including, when possible, the categories and the approximate number of data subjects affected, and the categories and approximate number of personal data records affected; (ii) the name and contact details of the data protection officer or other contact point where more information may be obtained; (iii) description of the possible consequences of the breach of personal data security and (iv) description of the measures adopted or proposed to remedy the breach of personal data security, including, if applicable, the measures adopted to mitigate the possible negative effects.

If it is not possible to provide the information simultaneously, and to the extent that it is not, the information will be provided gradually without undue delay.

11 Data Protection Officer (DPO)

If so required under article 37.1 of the GDPR, it must designate a data protection officer and communicate their identity and contact details to the DATA CONTROLLER, as well as complying with all the provisions of articles 37, 38 and 39 of the GDPR.

12 Disclosure of data to third countries

The DATA PROCESSOR may transfer personal data to a third country or an international organisation only if the processor has provided appropriate safeguards pursuant to article 46 of the GDPR, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.

15.6 Duty of non-disclosure

The DATA PROCESSOR hereby undertakes not to disclose information classified as confidential and facilitated by the DATA CONTROLLER in order to provide the services covered under this Agreement.

The non-disclosure obligation will be for an open-ended period, and will remain in force after the finalisation, on whatsoever grounds, of the relationship between the data controller and the data processor. Likewise, the DATA PROCESSOR will be responsible for ensuring that its staff, collaborators and all persons under its responsibility and who could have access to the confidential information and personal data of the DATA CONTROLLER respect the confidentiality of the information, as well as the

obligations concerning the processing of personal data, even once its relationship with the DATA CONTROLLER has concluded.

15.7 Duration

The processing of the personal data covered by this Agreement will extend throughout the entire contractual term.

15.8 Destination of the data at the end of the contractual relationship

Once the agreement and, therefore, the relationship resulting from the agreement between the DATA CONTROLLER and the DATA PROCESSOR has concluded, the latter will proceed to destroy the personal data of the DATA CONTROLLER.

The DATA PROCESSOR may keep, appropriately blocked, the personal data of the DATA CONTROLLER, for as long as any liabilities stemming from the relationship between both parties could arise.

15.9 Exercise of rights

The DATA PROCESSOR must forward to the DATA CONTROLLER any request for the exercise of the rights to access, rectification, removal, objection, restriction, portability and to not be the object of individualised automated decisions, made by a data subject whose data have been processed by the DATA PROCESSOR in compliance with this Agreement, to enable the DATA CONTROLLER to rule on the lawfulness of the periods established under prevailing regulations.

The forwarding of the request to the DATA CONTROLLER must be sent as expeditiously as possible, together, where appropriate, with other information that may be relevant to resolve the request.

Requests should be made in writing and sent to Paseo de los Olmos nº 19, 28005 Madrid, with the reference "Data Protection", accompanied by a photocopy of the user's national ID document, or by sending an email to: protecciondedatos@enagas.es.

Furthermore, the DATA PROCESSOR must process any instruction related to the aforementioned rights received through the DATA CONTROLLER, within the established deadline.

15.10 Subcontracting

The DATA PROCESSOR may subcontract with different suppliers to provide the services that are part of the subject matter of this Agreement and that involve the processing of personal data.

The DATA CONTROLLER consents to the subcontracting of suppliers for the normal provision of services.

The sub-processor, who will also hold the status of data processor, is also obliged to comply with the obligations established in this Agreement for the DATA PROCESSOR, as well as the instructions given by the DATA CONTROLLER. The DATA PROCESSOR will continue to be fully liable to the DATA CONTROLLER with regard to compliance with the aforementioned obligations.