

## GENERAL CONDITIONS OF WORKS

### 1. PARTIES.

Supplier (natural person or legal entity indicated at the top of the Order), and Enagás S.A. (or any of its Subsidiaries) (hereinafter "Enagás").

### 2. CONTRACTUAL REGIME.

The Order is governed by the terms and conditions set out in the Order and in the General Conditions.

These General Conditions will apply in full to the Order, except where they are expressly derogated from or modified in the Order.

In the event of any discrepancy between the General Conditions and the Order, the provisions of the latter will apply.

To be effective, any modification of the General Conditions or the Order must be formalised in writing and signed by the Supplier and Enagás.

Any exception to these General Conditions proposed by the Supplier will only be valid if it has been previously formulated in writing and accepted in the same form by Enagás, and will only be applicable to the Order for which it has been proposed, and under no circumstances may it be extended to current or subsequent contracts with the Supplier.

### 3. ENTRY INTO FORCE.

Once signed by Enagás, the period of validity of the Order will be extended until completion of the works contracted, including the guarantee period. For the issue and payment of invoices, the Order will come into force and take effect upon receipt by Enagás of the duplicate copy of the Order, accepted and signed by the Supplier.

### 4. PRICES AND EXTRAS.

The total amount of the Order is as stated in the Order and, unless otherwise stated in the Order, does not include VAT.

The prices included in the Order will be final, unless otherwise stated in the Order. Price increases or revisions to the prices indicated in the Order will not be accepted, unless they are contemplated in the Order.

Increases in work over and above those indicated in the Order will not be accepted unless they are contemplated in the Order or expressly authorised in writing by Enagás by means of a document signed by both Parties.

The Supplier will be responsible for any difference between the amount tendered and the actual cost incurred for the works.

### 5. EXECUTION PERIOD AND PENALTIES.

The Order will not be deemed to have been fulfilled, and therefore the works completed, until they have been constructed and assembled at the place and within the time limits specified in the Order and, where applicable, the relevant technical documentation requested in the Order has been delivered. At the same time, the provisional acceptance of the work will be deemed to have taken place by means of a document issued for this purpose by Enagás.

Whenever the Supplier does not comply with the deadline set out in the Order, and the delay is not attributable to Force Majeure or Fortuitous Event, as these are defined in the General Conditions, the Supplier will pay Enagás a cumulative penalty for each week of delay or part thereof, for the following amounts:

- For the first week of delay or part thereof: 0.5% of the total price of the Order.
- ☒ For the second week of delay or part thereof: 1.5 % of the total price of the Order.
- ☒ For the third week of delay or part thereof: 3% of the total price of the Order.
- ☒ For the fourth week of delay or part thereof and subsequent weeks: 5% of the total price of the Order, for each of these.

The penalties for delay cannot exceed, overall, 10% of the amount of the Order.

Once a cumulative penalty for delay totalling 10% of the total amount of the Order has been reached, Enagás may terminate the Order pursuant to the provisions set out in these General Conditions.

## 6. BILLING AND PAYMENT.

All invoices must be issued in compliance with current tax and commercial requirements.

Invoices issued for orders to which these General Conditions apply must include the following codes:

Order No./ Supplier/company code (Enagás company indicated on the order):

Certification No.: (8000xxxxxx that Enagás has previously had to provide to the Supplier).

Invoices must be issued with the same concepts or items indicated in the Order, without which they will be returned to the Supplier.

Invoices must be sent, for management on the Easyap platform, by one of the two alternative means, at the Supplier's discretion, indicated below (these addresses are exclusively for receiving invoices):

- Hard copy to Apartado de correos 3590 (PO Box).
- Electronic format (facturae 3.2.1 or higher) or PDF (version 1.3 or higher unprotected and with a resolution of 300Dpls or higher). In this case they will be sent to the following email address [facturasconpedido.enagas@easyap.com](mailto:facturasconpedido.enagas@easyap.com)

If invoices are sent in PDF format, they must meet the following requirements:

- Include only one file per invoice and never more than one invoice per PDF. In each email you can attach as many invoices and attachments as you want, but must always have different names. This means that the name of one PDF cannot be the root of another. For example, you cannot call one PDF 'invoice' and another 'invoice01' in the same email. The recommendation would be "I01.pdf", "I02.pdf", "I03.pdf", etc.
- If you wish to send attachments to the invoice, this must be done in an additional file and never together with the invoice. The file name of the attachment file must be the same as that of the invoice, followed by  
  
"\_attachment". For example: "invoice.pdf" and "invoice\_attachment.pdf", for the invoice and attachment file respectively.
- If you are going to send several invoices in the same email they can be sent in a compressed .zip file (.rar is not supported).

You can check the status of your invoices by registering at <https://proveedoresenagas.easyap.com>

Under no circumstances can the invoice date be earlier than the date the work is conducted.

Invoices will not be accepted if their prices and discounts do not match those set out in the Order, except in those cases in which, as a consequence of a review accepted by both Parties, or subsequent agreement, different prices and conditions are applicable.

Payment of invoices issued by the Supplier, in accordance with the provisions of the foregoing conditions and the Order, will be made on the day after 60 days have elapsed from the acceptance of Works, under the terms established in article 4 of Law 3/2004, of 29 December, which establishes measures to combat late payment in commercial transactions; and will be managed by "reverse factoring/transfer" by a bank of Enagás' choice. If, in accordance with the foregoing, the day on which payment is due to be made is a public holiday, payment will be made on the next working day.

The handover of the guarantees required in the Order from the Supplier to Enagás is an essential requirement for acceptance of the invoices.

Generically, for orders for amounts between 5,000 and 100,000 euros, Enagás will retain 10% of each invoice submitted by the Supplier as a guarantee on the amount to be paid in each invoice. The withholding of 10% of each invoice submitted by the Supplier will be returned at the end of the guarantee period referred to in General Condition 18.

The amounts paid will be considered, for all purposes, as payments on account of the final settlement, which will be made once all the works subject to this Order have been completed, without their payment prejudging the compliance of the same with the provisions of this Order.

## **7. SUPPLIER'S OBLIGATIONS.**

The Supplier will provide the works listed in the Order within the execution period specified therein, using the utmost diligence required in the professional field for the type of works covered by the Order, and in accordance with the usual practices of companies with proven experience, following the applicable procedures and standards and the instructions received, where appropriate, from Enagás.

In addition, the Supplier undertakes to comply with the quality level set out in the Order.

The Supplier undertakes to facilitate access to any other Supplier designated by Enagás and coordination with, for the rendering of works other than those object of the Order, but with which there may be any type of interrelationship.

The Supplier, where applicable, will be in possession of all permits and licences for the use of the tools necessary to perform the works which are the subject of the Order.

The Supplier will carry out the work in a diligent manner, subject to these Conditions, and will take special care in the conservation of the works, plans, documents, tools, utensils, materials and other objects, whether their own or those supplied by Enagás, and will be responsible for any damage that may occur.

The Supplier will be liable for all damages, including non-contractual liability, which the Supplier and the persons for whom it is legally or contractually liable may cause as a result of the execution of the works and/or which occur on the site of the works.

The Supplier will be liable to Enagás for the actions and/or omissions of subcontractors, as if it had done so itself.

The Supplier will be responsible for providing all the human resources necessary for the correct execution of works, as well as for ensuring that they have and receive the appropriate training to guarantee the fulfilment of the objectives. In this regard, the Supplier's personnel assigned to the execution of the works will be duly qualified and experienced in similar works.

The Supplier will be responsible for providing all the human resources necessary for the correct execution of the works, as well as for ensuring that they have and receive the appropriate training to guarantee the fulfilment of the objectives. In this regard, the Supplier's personnel assigned to the execution of the works will be duly qualified and experienced in similar works.

The Supplier must present supporting documentation confirming that it is up-to-date with its tax and Social Security obligations.

The Supplier undertakes to fulfil and ensure that its staff fulfil the obligations imposed by labour legislation in matters of occupational health and safety, social security, complementary pension plans, accident insurance and staff recruitment.

It also undertakes to comply with and enforce safety and behavioural rules and any standards implemented by Enagás in its facilities and plants and Enagás undertakes to supply these standards and any amendments that may occur during the provision of the works. In this regard, attached as Appendix 1 to these General Conditions is Enagás' policy on safety (personal safety, infrastructure, environment and road safety), health and well-being, the environment (promoting energy efficiency and reducing emissions) and quality, which the Supplier hereby declares to be aware of and accepts without prejudice to its compliance with any other obligations that may arise in this regard.

The Supplier will be responsible for any organisational, labour, disciplinary and social security matters and, generally, any responsibility arising in relation to the resources assigned to execution of the Works and no general labour and/or legal relationship will be established between the above-mentioned staff of the Supplier or its subcontractors and Enagás.

The Supplier, whose work is carried out at an Enagás site, undertakes, throughout the term of the Order, to remain registered on the Enagás Contractor Accreditation Service (SACE) platform under the terms contained in the Instructions attached as Appendix 2 to these General Conditions, which the Supplier declares to be aware of and accepts, as well as to provide during the same term any documentation on the protection of the health and safety of workers that may be required by Enagás for the purposes and under the terms of the provisions of Royal Decree 171/2004, of 30 January, which implements article 24 of Law 31/1995, of 8 November, on the Prevention of Occupational Hazards, in the area of coordination of business activities.

The Supplier will be liable and will hold harmless Enagás from any suit or claim initiated by the resources assigned to the execution of the works and/or imposed on Enagás as a consequence of said action.

With regard to infrastructure, the Supplier will provide the necessary physical space, for equipment that is not located at Enagás' facilities, for the provision of those works that do not require the physical presence of the Supplier's personnel at Enagás' facilities, within the scope of the service.

The Supplier will provide the technical means necessary for the provision of the works covered by the Order and will be responsible for the maintenance of such means. If, for safety reasons, the technical resources must be provided by Enagás, the cost of their use will be charged to the corresponding invoice.

Inscriptions substantiating that they have been carried out by the Supplier may be placed on the works, and the name of Enagás must also appear on them. No entry of a commercial advertising nature may be published without the prior formal written approval of the Party concerned. In any case, the Supplier will be subject to all indications received from Enagás.

The Supplier or its subcontractors may not publish articles, photographs or advertisements relating to the works covered by the Order without the prior approval of Enagás.

## **8. OBLIGATIONS OF ENAGÁS.**

Enagás will pay the price for the works in the manner and amount established in the Order.

Enagás will collaborate with the Supplier in the development of the works, facilitating access to the information requested by the Supplier.

With regard to infrastructure, Enagás will provide the necessary physical space at its facilities in those cases in which, due to the nature of the works provided or for security reasons, the physical presence of the Supplier's personnel is required for their execution. The use of this infrastructure will be charged for in the corresponding invoice.

## **9. OWNERSHIP AND POSSESSION.**

Both the works and the site where they are developed are the exclusive property and/or right of Enagás and, consequently, the Supplier does not acquire any ownership rights over them nor may it constitute any real right over them. The Supplier expressly waives any right of retention on the works.

The ownership of the materials supplied by the Supplier shall be transferred to Enagás at the time these are received at the work site.

Likewise, all designs, plans and specifications delivered by Enagás to the Supplier for the execution of the works belong to Enagás, as well as inventions, patents, utility models and other industrial property rights generated or to be generated on the basis of any documentation delivered by Enagás to the Supplier for the execution of the works.

Possession of the works will remain with the Supplier until Provisional Acceptance, at which time the associated risks will be transferred to Enagás.

The ownership of the materials to be supplied by Enagás, where applicable, will remain with Enagás throughout the term of the Order. Notwithstanding the foregoing, the risk on the same will remain with Enagás only as long as they are not delivered to the Supplier where indicated in the Order, and the Supplier will, from this moment, be liable to Enagás for any damages caused to the same, except those arising from manufacturing defects.

## **10. DOCUMENTATION.**

At the time of completion of the provision of works, or, failing this, at such time as the Parties may agree, the Supplier will send Enagás the technical documentation required in the Order, free of charge.

The Order will not be considered completed until all the documentation required in accordance with these General Conditions and the Order itself has been received by Enagás. Delays in the delivery of the requested documentation will entitle Enagás to withhold payments to the Supplier until such documentation is received.

The Parties undertake, for a minimum of six (6) years from the date of receipt of the works (according to General Condition 5) and of the documentation, to keep in their possession the original documents, as well as any other document deemed appropriate from an inspection and quality control point of view, and also undertake to provide each other with the necessary copies for the same period of time.

## **11. ASSIGNMENT.**

Enagás and its Group companies may convey, on a singular basis and through any act in the law, its position in this Order to any other company that forms part of the ENAGÁS Group. Likewise, ENAGÁS and the companies of its Group may convey their contractual position as a consequence of any universal transfer (including, but not limited to, those arising from mergers, splits, segregation and global transfer of assets and liabilities), whether such universal transfer is voluntary, or as a consequence of the application of electricity or gas sector regulations on the legal separation of activities. Enagás or its Group company will communicate, as soon as possible, the effective date of the transfer and the identification data of the new Party to this Contract.

The Supplier cannot assign or transfer the benefits, rights, interests, obligations and contractual position stemming from the Order in full or in part without prior written consent from Enagás. Breach of this obligation by the Supplier will be sufficient cause for the termination of the Order.

The assignee will in any event assume in full all rights and obligations arising from this Order, whether before or after the time at which the assignment becomes effective.

## **12. SUBCONTRACTING.**

The Supplier may not subcontract all or part of the Order without the prior written approval of Enagás. Failure to comply with this obligation will entitle Enagás to terminate the Order.

No contractual and/or labour relationship whatsoever will arise between Enagás and the Supplier's subcontractors as a consequence of the execution of the Order.

Enagás reserves the right to request the substitution of those subcontractors that, prior to the commencement or during the progress of the Order, are not reasonably appropriate to maintain. The Supplier may ask Enagás to give reasons for requesting replacement of the subcontractor.

The subcontracting will not exonerate the Supplier from any of its contractual responsibilities or obligations. The Supplier will also be fully liable with Enagás for the acts, faults and negligence of any of its subcontractors, or of their agents and workers.

Enagás will not be liable to any subcontractor or any personnel of the subcontractors with regard to any claim.

The Supplier shall hold Enagás harmless from any claims that subcontractors may lodge with regard to this Order, compensating Enagás for any cost or payment which, where appropriate, it is obliged to make as a consequence of said claims, including the legal defence and procedural representation.

In the event of a claim by any subcontractor, Enagás will be entitled to withhold the amount claimed by them from the invoices pending payment to the Supplier.

### **13. INTELLECTUAL AND INDUSTRIAL PROPERTY.**

The Supplier guarantees Enagás that it holds the intellectual property rights to the products it offers, either directly or indirectly through the corresponding agreements with its suppliers. In any case, the Supplier will be responsible for obtaining the necessary assignments, permits and authorisations from the holders of the corresponding patents, models and trademarks, as well as for obtaining the necessary licences or intellectual property rights, and will be responsible for the payment of the rights and compensation derived from such concepts.

The Supplier will at all times protect Enagás from any liability for infringements related to rights arising from patents, trade secrets, copyrights, trademarks, trade names or similar rights and, ultimately, from any liability for infringements related to industrial or intellectual property rights that the Supplier may incur. The Supplier undertakes to do whatever is necessary to indemnify Enagás and its personnel against any claims or lawsuits that may be brought against Enagás and/or its employees for such infringements and to indemnify the latter for all damages, expenses and costs (including consultancy, legal and lawyers' fees) that it may incur as a result of such claims or lawsuits or for the actions in which it is required to intervene.

For the purposes of the foregoing, the Supplier undertakes to notify Enagás, in an irrefutable manner and immediately upon receipt, of any claim, judicial or out-of-court, addressed to it and filed by third parties with respect to the industrial or intellectual property rights that are the object of the Order.

In any event, if Enagás is sued by a third party for breach by the Supplier of the obligations referred to in this clause, the Supplier, at the request of Enagás and within ten (10) calendar days, will be obliged to present a financial guarantee for a minimum of ten percent (10%) of the total amount of the Order and its revisions, extensions and administrative work, if any, to cover the amount of the claim received.

Enagás will own all documents, designs, plans, computer programs and specifications, as well as their analogue versions and any copies thereof that Enagás may deliver to the Supplier for the execution of the work, as well as any inventions, patents, utility models and other industrial property rights generated or that may be generated on the basis of any documentation that Enagás may deliver to the Supplier for the execution of the work. The Supplier must use them exclusively for the execution of the Order and will return them on completion of the same, maintaining at all times the appropriate precautions for the processing, handling and transmission of the information, guaranteeing security and confidentiality, in accordance with the provisions of these General Conditions and the legislation in force applicable to each Order.

Designs, documents, plans, computer programs and specifications, as well as the analogue versions and copies thereof, owned by the Supplier before the start of the Services, are and will remain the property of the Supplier, and the Company will not have any right over or interest in them except for the receipt of the Services. Likewise, the Supplier owns the designs, documents, plans, computer programs and specifications, as well as the analogue versions and copies thereof, generated where appropriate using its own documentation and technology in the execution of the Works, as well as inventions, patents, utility models and other industrial or intellectual property rights. However, the designs, documents, plans and computer

programs (including their methodology, processes, technologies, hardware, licences or algorithms), as well as their analogue versions and copies thereof, which have been delivered by the Supplier in compliance with the Order, will become the property of Enagás.

In any case, the intellectual or industrial property rights and the technology and methodology resulting from the works or services carried out by the Supplier in compliance with the Order, as well as the registrations to which any of these give rise, will correspond to Enagás, without this conferring any right on the Supplier to increase the price set in the Order for said work or service.

Furthermore, neither of the parties may use the registered trademarks or trade names of the other party in public communications without their explicit formal approval.

#### **14. ORDER TERMINATION.**

The Order may be terminated on any of the following grounds:

- a) At the request of either Party, in the event of a major breach by the other Party, in full or in part, of the obligations set out in the Order when, having been requested by the Party not in breach to redress the Breach, wherever possible, this has not taken place within a deadline of 10 calendar days.

For the purposes of this Condition, the accumulation by the Supplier of a late payment penalty equal to or greater than 10% of the total amount of the Order, as well as the non-renewal of the guarantees upon their maturity in case of need, as indicated in General Condition 15, will be considered non-fulfilment.

- b) At the request of Enagás, without the need to identify just cause, provided that the Company is notified one month in advance.

In the cases of termination set out above, the following effects will take place:

In case a), the Party in breach will be obliged to compensate the other party for the damages and losses caused as a result of the breach, including extra costs caused by breach of the Order.

In case b), Enagás will pay the Supplier all amounts pending payment and, following an agreement between the Parties to this end, will settle any costs which it had incurred prior to notification of the termination and which were directly attributable to the Order.

Furthermore, in cases a) and b), when the Supplier receives notification of early termination of the Order, it will discontinue all related works and will provide all means within its power to cancel any outstanding orders and subcontracts, under terms that are satisfactory for Enagás, and limiting itself from that time to performing the services required to safeguard and protect the services in progress and everything related thereto.

Likewise, for the purposes of this General Condition, the other causes for termination of the Order will be considered to be those contained in these General Conditions and those provided for in the legislation in force.

#### **15. LIABILITY.**

The Supplier will be liable to Enagás for any damages that the Supplier itself and the persons for which it is legally or contractually responsible, may cause to Enagás or its employees, resulting from an action or omission by the Supplier in the fulfilment of its obligations or by any of the aforementioned persons, involving any kind of negligence, fault or fraud.

The Supplier's aggregate total liability to Enagás arising from a given Order, in relation to all guarantees and indemnities for damage to Enagás' property, may not exceed, except in the case of wilful misconduct or gross negligence or any other type of liability that cannot be excluded or limited by law, 100% of the amount of the Order or the amount required as a minimum limit of indemnity agreed by the Parties for the Order, in the event that such amount is greater. Exceptions to this limit are engineering redesign, compensation for damages to third parties, and penalties for delays in complying with the Order.

In the event of contributory negligence, or the involvement of a third party in causing damages, liabilities will be determined proportionately, based on the degree of involvement of the Parties.

Liability for indirect, consequential damages and harm caused by one Party to the other is excluded (in particular, losses of production, operation and profits are excluded, and, in general, losses or damages of an indirect nature that each Party may have suffered).

The Supplier will be liable for and will hold Enagás harmless from any third party claims against Enagás for damages caused to said third parties resulting from an action or omission in the fulfilment of its obligations by the Supplier or by any of the persons mentioned, involving any kind of negligence, fault or fraud. For these purposes, third parties will be understood to refer not only to legal and physical persons not parties to this Order, but also to the employees of Enagás, and the Supplier must be liable for any damages that may be caused to them. The same liability may be demanded of Enagás by the Supplier, except for claims for death or accident of the Supplier's employees or its dependent personnel, in which cases the Supplier will be liable, and Enagás will be held harmless and exempt in relation to such claims.

The Supplier's liability will not be limited as a consequence of documents or information provided by Enagás for the performance of the object of the Order, unless this information conditions or is the basis for the performance of said order.

The Supplier will be liable to third parties, and Enagás will be exempt from all claims for death or accident of its employees or its dependent personnel, as well as those raised by third parties arising or resulting from accidents, actions or omissions by the Supplier due to non-compliance with the obligations of the guarantee period included in General Condition 18.

In the event of termination of the Order due to non-fulfilment by the Supplier, the latter will indemnify Enagás for the extra costs incurred by the latter for new works contracts. To cover this compensation, Enagás may take possession of the amounts withheld or, where appropriate, execute the performance bond, as established in General Condition 15 below.

## **16. GUARANTEES AND WITHHOLDINGS.**

For those orders in excess of 100,000 euros or for those orders for which this is expressly stipulated in the Order, upon signing the Order and prior to the commencement of the works, the Supplier will provide Enagás with a bank guarantee, as a performance bond for compliance with the obligations and responsibilities arising from the Order, for a value of 10% of the price and in accordance with the template attached in Appendix 3 of these General Conditions. The guarantee obligation by means of a guarantee for said value will remain in force in favour of Enagás during the entire guarantee period established in General Condition 19 to cover damages and expenses that may arise from defects in the works provided; and the guarantee will be returned at the end of said period if these defects do not exist.

If the duration of the order is increased during its execution, the Supplier will be obliged to maintain in force the guarantee already provided to Enagás when the Order was signed, with the same requirements as those set out above.

The guarantee and performance bond shall be issued until the date on which the guarantee period is deemed to end. In the event that the guarantee period ends after the date indicated in the guarantee, the Supplier will be obliged to extend the validity of the guarantee (or to provide a new guarantee) until the new estimated end date of the guarantee period indicated by Enagás. Failure to extend the validity of the guarantee (or failure to provide a new guarantee) will be considered a breach of the Order.

Both the performance bond (where applicable) and the withholdings carried out may be used to refund the amounts accrued, for compensation for delays, as well as any liability that the Supplier and/or its subcontractors could incur as a consequence of any breach of the obligations assumed pursuant to this Order.

The bank guarantees indicated in these General Conditions must be issued (i) by a Bank of recognised prestige with a commercial branch in Spain and a credit rating of at least BBB by Standard & Poor's or equivalent by Moody's or Fitch, and (ii) with the validity, scope and amount determined in the templates attached to the General Conditions and in the Order. Enagás reserves the right to request the replacement of the guarantees if the Bank's credit rating is downgraded during the formalisation or execution of the Order. The Supplier will bear the costs arising from the guarantees.

An essential requirement for the payment of invoices will be the delivery by the Supplier to Enagás of the guarantees required by the latter in accordance with these General Conditions or in accordance with the Order. In the case of a hard-copy guarantee, please send it to the following postal address:

ENAGÁS.

Paseo de los Olmos,19.

28005.Madrid.

FAO: Jhoanna Kalilá Aldana Jiménez.

Digital Finance Services Center Management.

If the guarantee is with a digital certificate, please send it to the following email address:

[DFSC.AVALES.PROVEEDOR@enagas.es](mailto:DFSC.AVALES.PROVEEDOR@enagas.es).

## 17. NO EMPLOYMENT RELATIONSHIP.

For the purposes of the Order, under no circumstances will the employees, agents or independent personnel reporting to the Supplier or its Subcontractors be considered related to Enagás.

## 18. INSURANCE.

The Supplier will take out and maintain in force, at its own expense, for sufficient sums assured and for the duration of the Order, the following Insurance Policies:

- a) **Social Security and Life and/or Accident Insurance** for all employees assigned to the work, pursuant to the Law.
- b) **Civil Liability Insurance** to cover third party claims for material or personal damages and their consequential damages caused while fulfilling the obligations set forth in the Order.

This Policy must include the following:

- 1) Enagás and its personnel, as well as any subcontractor of the Supplier involved in the execution of the Order, will be included as additional insured parties in said policy, without losing their third party status.
  - 2) The indemnity limit shall have a minimum coverage of €500,000 and may be increased, on objective grounds, in the Conditions of the Order.
  - 3) In addition, the insurance policy will include the guarantees for Civil Liability arising from Accidental Pollution of the Environment, Pre-existing Property, Adjoining Property and Work on third party premises. Employer's Liability to the Supplier's employees or those of its contractors and Product Liability and Post-Work Liability.
- c) **Material Damage Insurance** on all vehicles, equipment, machinery and tools used. These insurance policies must also cover Civil Liability for damages that its vehicles, equipment and machinery could cause to Enagás or to third parties.

These Policies will act as "Primary Policies" and always in the first instance before any others that may be applicable. The Insurance policies indicated must be taken out with Insurance Companies of recognised solvency and prestige.

Notwithstanding the foregoing, the Supplier may, at its own expense, take out any supplementary insurance policies deemed appropriate for full coverage of its liabilities under the Order.

Prior to the commencement of works, the Supplier shall send Enagás a certificate of each of the insurance policies indicated in the previous paragraphs and which will be attached as Appendix 4. This certificate must be renewed annually prior to its expiration, with an undertaking to extend the range of cover, if deemed necessary by Enagás. Failure to comply with this obligation will result in the blocking of the payment of the contract's invoices, until they are delivered in accordance with the Order.

This certificate will expressly contain at least:

Validity period;

Contracted limits;

Coverage contracted

The Supplier is obliged to inform Enagás in writing of any incident during the validity of the Order affecting the validity and conditions of the insurance policies taken out.

Enagás may at any time ask the Supplier to provide the originals of the Policies, or certified copies, of the insurance cover it has taken out, as well as any receipts or proof that the payments of the corresponding premiums are up to date.

In the event of a loss event, any difference that arises in payment of the compensation, whether through the application of an excess policy or for any other reason, with regard to the insurance policies taken out, will be payable by the Supplier.

All insurance policies taken out will include a statement exempting from liability and express waiver of the right of recourse established in article 76 of the Insurance Contract Law in Civil Liability policies and subrogation in damage policies on the part of the insurer against ENAGÁS.

The Supplier, under its sole responsibility, will require its subcontractors to take out the necessary insurance policies. This will not exonerate the Supplier from its liability to Enagás.

Breach of this clause will be sufficient grounds for contract termination.

The insurance certificate must be sent to the following email address [DF.SEGUROS@enagas.es](mailto:DF.SEGUROS@enagas.es).

## **19. WARRANTY PERIOD.**

A warranty period of 24 months is established for the works from the provisional acceptance of the works to their completion, in accordance with the provisions of General Condition 5. Once this period has elapsed, the works will be deemed to have been definitively accepted, with Enagás issuing the corresponding document, except as established in the following paragraphs.

If, within said warranty period, the works are found to be defective or in any way in breach of the Order, Enagás will notify the Supplier in writing of the defects or breaches observed.

From such notification and during the warranty period, the Supplier shall, at its own expense, re-perform all works necessary to correct any errors or omissions in the performance of the same.

A new warranty period equivalent to the previous one will be applicable to those works that have been subject to repair or replacement as a consequence of the provisions of this General Condition.

In the event that, where defects exist, the Supplier fails to comply with its obligation to repair or replace such works as established in these General Conditions, Enagás may repair or replace such works at its own expense, charging the Supplier for the costs it has incurred. This is without prejudice to Enagás' right to be compensated itself for the expenses, damages and losses that this may have caused it, and to enforce, where applicable, the performance bond established in General Condition 15, or to make the withholdings established therein its own.

Ç

**20. TAXES.**

All taxes and fees will be charged to the Party to which they correspond pursuant to current legislation. When the

Supplier is a foreign company, it must provide the certificate of tax residence, for the purposes of the application of the relevant double taxation avoidance treaty

**21. CONFIDENTIALITY.**

For the purposes of the Order, Confidential Information will mean all information delivered, sent, received or exchanged, identified as such, in particular, plans, drawings, designs and specifications, except as expressly authorised for disclosure in writing by each Party.

Confidential Information may not be disclosed to third parties or used for purposes other than those for which the Order is made during the term of the Order and for an additional five years after its termination, except as provided in this General Condition.

The content of the Order may not be publicly disclosed by either Party without the prior written consent of the other Party.

Confidential Information will not include any information:

- that was in the public domain at the time of disclosure.
- which, following disclosure, is published or otherwise enters the public domain, without breach by the Party receiving such information.
- that, at the time of disclosure, the Party receiving such information was already in possession of it.
- which, following disclosure, was received from a third party who has a legal right to disclose such information; or
- that was independently developed by the receiving Party without reference to the Supplier's Confidential Information.

In addition, either Party may disclose Confidential Information of the other Party if required to do so by law or by court order.

In the event of any disclosure or loss of Confidential Information, the receiving Party will promptly notify the supplying Party.

Any type of information, verbal or written, that Enagás may provide to the Supplier will be understood to be the exclusive property of ENAGÁS. The Supplier undertakes to use said information exclusively within the scope of the provision of the contracted works and for the sole purpose of complying with them as agreed, and will consequently be liable for any damages that may arise for Enagás as a result of non-compliance with the foregoing.

Upon completion of the Order, the Supplier undertakes to delete from its files and remove from its facilities all information belonging to or provided by Enagás, and not to disclose it itself or through third parties. Enagás will also have the right to carry out on-site verification that the above actions have been carried out by the Supplier.

When the personnel providing a service without access to confidential information have access to premises, media or resources containing personal data or any other kind of confidential documentation belonging to ENAGÁS, the PROVIDER will inform its personnel of the prohibition of access and, in the event of incidental access, the obligation not to disclose said information.

Unless express authorisation is granted or a contract is signed for the processing or release of personal data (see ANNEX 8), the PROVIDER is expressly prohibited from accessing the personal data owned by ENAGÁS. The PROVIDER undertakes to inform its personnel of this prohibition and observe due professional secrecy and confidentiality with regard to any information of a personal and/or confidential nature unrelated to the provision of the service to which they may incidentally have access.

## **22. FORCE MAJEURE.**

Neither Party will be responsible for the breach of its contractual obligations as a consequence of Force Majeure or a Fortuitous Event, as defined in the Civil Code. Any instances of Force Majeure or a Fortuitous Event will be communicated to the other Party no later than 48 hours after its existence has become apparent.

Each Party will use its best efforts (to the best of its ability) to avoid or mitigate

the effects of a situation of Force Majeure or Fortuitous Event, as well as to ensure the normal continuation of the Order.

In these cases, the deadlines for compliance with the obligations stipulated will be extended for a period that is equivalent to the time lost as a consequence of Force Majeure or a Fortuitous Event.

If the situation of Force Majeure or a Fortuitous Event that affects all of the obligations of one of the Parties with regard to this Order, or a major part of its obligations, lasts uninterruptedly for more than two months, the Party not affected by this situation of Force Majeure or a Fortuitous Event may terminate this Order by giving fifteen (15) calendar days' notice. Where appropriate, the termination will not exonerate the Party from compliance with the obligations that arose prior to the situation of Force Majeure or the Fortuitous Event.

## **23. APPLICABLE LAW AND JURISDICTION.**

The law applicable to the Order will be Spanish law.

The Parties hereby undertake to comply with the Order 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 Order, 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 the Order.

## **24. QUALITY ASSURANCE AND ENVIRONMENTAL REQUIREMENTS.**

ENAGÁS may require the Supplier to have a properly documented quality assurance programme, devised based on UNE-EN-ISO 9001 guidelines, and it must be applied to the subject matter of the Order. In addition, if necessary, it may require the development of a specific Quality Plan for the order, in accordance with ISO 10005 "Quality Management. Guidelines for Quality Plans".

This Contract will be governed by the applicable environmental legislation in force, both state, regional and local, as well as the internal regulations of ENAGÁS in this respect defined in its environmental management system and the commitments acquired by the supplier within the framework of its activity.

Where applicable, the supplier must comply with the environmental and energy efficiency requirements for contractors and suppliers of ENAGÁS specified in Appendix 5 Environmental Protection.

## **25. SUSTAINABILITY.**

The supplier guarantees and acknowledges the importance of adhering to ethical and sustainability obligations and principles in the conduct of their business.

Without prejudice to the regulatory and legal provisions applicable to each of the Parties, in all matters relating to the development and execution of this Agreement, the Supplier guarantees that all directors, managers and employees will act in accordance with the principles laid down in the ENAGÁS Group Code of Ethics (published on the following link on the ENAGÁS website), [http://www.enagas.es/enagas/es/Sostenibilidad/Codigo\\_etico\\_y\\_politicas](http://www.enagas.es/enagas/es/Sostenibilidad/Codigo_etico_y_politicas), or others that the supplier has established as its own, provided they are equivalent to those set out in the ENAGÁS Code of Ethics.

Furthermore, during enforceability of the Agreement, the Supplier undertakes to allow ENAGÁS to audit the level of compliance with these requirements, and accepts any possible corrective or preventive measures that may be introduced.

## **26. PREVENTION OF CORRUPTION**

The Parties agree that, throughout the period in which the order is in force, they will comply with, and take reasonable measures to ensure that they, their directors, officers, employees subcontractors and agents and other third parties under their control or determining influence also comply with, all the applicable domestic and international standards aimed at the prevention of bribery and/or improper payments, money laundering, terrorism financing or other unlawful activities, or any other rules or regulations aimed at the prevention of corruption that may also apply to them, including, but not limited to, the UK Bribery Act and the United States Foreign Corrupt Practice Act (FCPA).

For the purposes of the preceding paragraph, the Parties agree that they will not, directly or indirectly through any of their employees, officers or agents, offer, promise, deliver, authorise, request or accept any undue benefit, financial or otherwise (or insinuate that they will or may do so at any time in the future) to/from the Competent Authorities (as defined below), or public or political party candidates or officials or persons acting on behalf of any of the above, or any other public officials, or any other person or company. Furthermore, the Parties undertake to take reasonable measures to prevent the materialisation of the conduct outlined above. In this regard, ENAGÁS hereby informs you that it has a Policy to combat fraud, corruption and bribery available via the following link on the ENAGÁS website:

[enagas.es/content/dam/enagas/es/ficheros/conocenos/etica-integridad/Politica-contra-el-fraude-la-corrupcion-y-el-soborno-ESP.pdf](http://enagas.es/content/dam/enagas/es/ficheros/conocenos/etica-integridad/Politica-contra-el-fraude-la-corrupcion-y-el-soborno-ESP.pdf)

The term "Competent Authority" refers to and includes all public and regulatory bodies, agencies, departments and entities, located in Spain or otherwise, that are competent in relation to the Order.

## **27. NON-EXCLUSIVITY.**

ENAGÁS will not be bound vis-à-vis the Supplier by any exclusivity agreement with respect to the works covered by these General Conditions or with respect to possible additional works, of any nature, that it may be interested in contracting.

## **28. DUTY OF MUTUAL INFORMATION BINDING THE PARTIES THAT SIGN THE ORDER**

In accordance with Organic Law 3/2018 on the Protection of Personal Data and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), the legal representatives of the parties involved in the order are informed that their identification or contact data included in this order or those provided on the occasion of the contractual relationship will be included in separate processing logs, the purpose of which is to manage the contractual relationship to perform the procured service, which is the legal basis that legitimises the processing of the parties' personal data.

The data collected are those that are essential for the establishment and development of the contractual relationship, and they will not be disclosed to third parties, unless there is a legal obligation to do so, having previously informed their owner. However, in the event that a service has to be performed by a third party, only third parties that are legally or contractually bound to the parties for the provision of the ancillary services required for the normal functioning of the service may access their personal data.

Each of the parties will retain the personal data of the representatives of the other party while this order is in force and, once the order has been fulfilled, they will be kept, duly blocked, at the disposal of judges and courts, the Public Prosecutor's Office and the competent Government Authorities, for the purpose of demanding any liabilities arising from the processing during the limitation period thereof (generally speaking, for six years in the case of accounting documentation and up to ten years for tax matters).

No international transfers of the representatives' personal data outside the European Economic Area will be made. Otherwise, the parties will inform each other in advance and comply with the necessary adequacy safeguards in accordance with the GDPR.

Similarly, they undertake to take the technical and organisational measures required to prevent any loss, misuse, alteration, unauthorised access or theft in order to guarantee the security of the personal data provided.

The legal representatives of each party may freely grant their rights of access, rectification, objection, erasure, portability and restriction of the processing to the other party, whenever applicable, by writing to the address indicated in the Order for notification purposes or by sending an email to [protecciondedatos@enagas.es](mailto:protecciondedatos@enagas.es) in the case of ENAGÁS and the address indicated by the PROVIDER in the order. In any event, this correspondence must include, among other information, the full name of the applicant, as well as the request upon which the application is based, and the address for notification purposes, in addition to the date, signature and photocopy of the applicant's National Identity Card or Passport.

The Parties undertake to inform each other of any changes to their data in writing.

If the parties have reason to believe that their data are not being processed properly, they may also send their claims to the Authority with competence in the area of data protection, namely the Spanish Data Protection Agency ([aepd.es](http://aepd.es)) in Spanish territory.

---

Signed in witness whereof, dated \_\_\_\_\_ of \_\_\_\_\_ of \_\_\_\_\_.

---

**BY THE PROVIDER**

---

**BY ENAGÁS**

**APPENDICES:**

- 1. HEALTH AND SAFETY, ENVIRONMENT AND QUALITY ASSURANCE POLICY**
- 2. CBA PROCEDURE: SACE Instructions.**
- 3. PERFORMANCE BOND TEMPLATE.**
- 4. INSURANCE CERTIFICATE TEMPLATE.**
- 5. ENVIRONMENTAL PROTECTION.**
- 6. CYBERSECURITY**
- 7. DATA PROTECTION**

**APPENDIX 1: HEALTH AND SAFETY, ENVIRONMENT AND QUALITY ASSURANCE POLICY**

The Supplier declares it is aware of and accepts compliance with the Health & Safety, Environment and Quality Policy, published in the following link on the ENAGÁS website:

[https://enagas.es/stfls/ENAGAS/Documentos/Políticas/Política\\_de\\_seguridad\\_y\\_salud\\_medio\\_ambiente\\_y\\_calidad.pdf](https://enagas.es/stfls/ENAGAS/Documentos/Políticas/Política_de_seguridad_y_salud_medio_ambiente_y_calidad.pdf).

## APPENDIX 2: CBA PROCEDURE: SACE INSTRUCTIONS

Enagás is committed to complying with and enforcing compliance with the established regulatory framework for occupational health and safety, involving not only its own professionals but also the contractors it works with. SACE is a tool which is already internationally consolidated and implemented in the petrochemical industry, where it has been well accepted.

Through the implementation of SACE, Enagás seeks to guarantee the availability of all procedures, ensuring that all processes are of high quality and that there is smooth and continuous communication between companies operating in the gas sector, in order to uphold the highest levels of safety.

The aim is to instil a common health and safety culture at all contractor companies and at all levels of contracting Enagás requires that all professionals take on board its health and safety policy and apply it in their daily operations. Safety should be second nature, both for Enagás and its supplier companies.

Therefore, in order for your proposal to be considered in this process, you are required to apply for registration on the Enagás Contractor Accreditation Service (SACE) by submitting the initial health and safety documentation requested for the Coordination of Business Activities procedure (Spanish Royal Decree 171/2004). The certificate issued by SACE, with a PASS qualification, must be attached to the Technical Bid documentation.

Presentation of the SACE certificate with a PASS is a specific requirement if your company is to be awarded the contract for the required service. Failure to present this SACE certificate will result in the exclusion of your proposal/bid from the process.

The platform for registration is:

<http://www.enagas.es/enagas/es/Proveedores/CoordinacionActividadesEmpresariales> or <https://enagas.sacegas.com/>.

At the start of the registration process, SACE, as the Coordination of Business Activities manager, will require an additional payment, valid for one year (VAT not included):

- €70 for a large company
- €60 for an SME
- €40 for a micro-enterprise
- €20 for the self-employed (1 person)

**If you are awarded** under this process, your company must maintain the PASS qualification for the duration of the bid/contract as a contractor. This will require regular updating of the information and documentation submitted to SACE. The annual cost (excluding VAT) of this platform for companies awarded contracts is as follows, minus the amount paid in advance (as indicated above):

- €232.7 for a large company
- €186.8 for an SME
- €121.9 for a micro-enterprise
- €73.8 for the self-employed (1 person)

As you know, contractor companies must submit a set of required documents in order to work with Enagás. SACE is intended to speed up this process: the necessary documents can be uploaded onto the platform for validation and a pass will be issued in return.

The pass is a card that must be presented by workers to access all Enagás facilities. Its authenticity can be verified by SACE or by a QR code. The annual cost of the pass is €50.3 per person, valid for two years.

Any vehicle or machinery entering Enagás facilities must also be registered in SACE. The annual cost (excluding VAT) for these items will be as follows:

- From 1 to 10 vehicles per company: €25.78 per vehicle (plus VAT);
- From 11 to 25 vehicles per company: €20.62 per vehicle (plus VAT). This rate will apply starting from the 11th vehicle;
- More than 25 vehicles per company: €15.47 per vehicle (plus VAT). This rate will apply starting from the 26th vehicle.

For example, to calculate the cost for 12 vehicles: the first 10 will be charged at €25.78 each, and the next 2 at €20.62 each. All amounts are annual and VAT excluded.

You can use SACE to consult your documentation and your position in the company health and safety ranking, among other operations.

In compliance with Article 10.2 of RD 171/2004, contractors are responsible for any necessary subcontracting and for passing on the information regarding risks, preventive and emergency measures, and instructions issued by Enagás. Likewise, contractors are responsible for asking subcontractors to register on the SACE platform.

Please note that, during the validity of the order, the aforementioned prices (applicable throughout the year 2025) will be updated at the beginning of each calendar year, based on the variation of the National General Consumer Price Index (IPC) experienced during the year prior to 2024. The next update will take place on January 1st, 2026, applying the variation of said index between December 2023 and December 2024, and so on in subsequent years.

**APPENDIX 3: PERFORMANCE BOND TEMPLATE**

THE BANK \_\_\_\_\_, represented by \_\_\_\_\_, who is aware of the Contract \_\_\_\_\_ (specify), executed by and between Enagás, S.A. (hereinafter "Enagás") and \_\_\_\_\_ (contractor)

**HEREBY GUARANTEES**

Irrevocably, in a joint and several, abstract manner, with express waiver to the guarantor's right to be liable only for his proportionate share of the debt ("beneficio de división"), to have all remedies first exhausted against the principal debtor ("beneficio de orden"), and to compel the creditor to sue the principal first ("beneficio de excusión"), being enforceable on first demand by Enagás, to \_\_\_\_\_ (Secured Company) up to a limit of \_\_\_\_\_ (Amount), as a definitive bond and assurance of performance of the obligations under the aforementioned Contract and, therefore, including the present and future liabilities arising therefrom.

The Bank will pay and enforce this guarantee up to its maximum and prefixed amount of \_\_\_\_\_ (Amount), on simple demand by Enagás, without such payment prejudging the resolution of disputes that may arise between Enagás, S.A. and \_\_\_\_\_ (guaranteed Company).

This guarantee will be fully valid until Enagás authorises its cancellation by registered letter to the Bank \_\_\_\_\_ returning this document, or until XX-XX-XX, the date on which it is estimated that the Guarantee Period of the aforementioned Contract will have ended, whichever occurs earlier.

The signatories to this Guarantee are duly authorised to represent and bind the entity that is underwriting, as stated in the power of attorney attested to by the notary public \_\_\_\_\_ on [ddmmyyyy] under Record No. \_\_\_\_\_.

This guarantee has been registered on today's date in the special guarantee register under number \_\_\_\_\_.

Signature and seal

**APPENDIX 4: INSURANCE CERTIFICATE TEMPLATE**

[Name], on behalf of and in representation of (Name of the Insurance Company), by virtue of the powers conferred through a public deed authorised in the presence of the Notary Public of [place], [name of Notary Public], on [ddmmyyy], under his/her record number.....

**HEREBY CERTIFIES:**

That the Company (Name of the Successful Bidder), has arranged with this Insurance Company (if there are several Insurers, please refer to each one of them and the percentage of participation in the insurance) a General Civil Liability cover through the contract/policy no. ...., in which from zero hundred hours of (ddmmyyy) and until twenty-four hundred hours of (ddmmyyy), the Civil Liability (expressly state: the different coverages that are required in the insurance clause of the Order \*) of (name of the successful bidder), in the performance of its activities, and with a limit in no case lower than 500,000 Euros.

This Certificate is issued for information purposes only and does not confer on the applicant any rights other than those set out in the policy. The rights and obligations of the parties are governed by the terms of the policy and the supplements issued. This Certificate does not modify, extend or enlarge the coverage agreed by the contracting parties in the aforementioned policy.

And in witness whereof and to be effective against whom it may concern, this Certificate is issued, in .....

Signature and seal.

(It must be signed by the Insurer)

## APPENDIX 5: ENVIRONMENTAL PROTECTION

### ENVIRONMENTAL AND ENERGY EFFICIENCY REQUIREMENTS FOR ENAGÁS CONTRACTORS AND SUPPLIERS

#### Compliance with current environmental legislation

Companies contracted to carry out works or refurbishments of various kinds undertake to comply with current environmental legislation when carrying out their activities within the work areas or when handling equipment, materials, products and waste.

With respect to the supply of products and services, the supplier undertakes to comply with the environmental laws in force regarding the use of hazardous or prohibited substances, packaging and labelling, transport conditions, noise and odour emissions during the operation of the equipment and any other environmental regulations established in the laws in force.

When supplying chemical products, the supplier will provide the safety data sheets for the products concerned by the order, which will contain the information described in the applicable legislation.

#### Use of materials, products, facilities and services

Will only use, at Enagás' facilities or service provision sites, the quantities of hazardous products that are strictly necessary for the performance of activities.

Will appropriately transport any material, product or equipment that is necessary for the development of the activity to the areas where it is to be used, taking responsibility for its temporary storage in the agreed places and for its safekeeping.

Will identify all hazardous product packaging in terms of its hazardousness, in accordance with the applicable legislation.

Will adopt the appropriate measures when handling chemical products, such as oils, greases, paints, solvents, etc., to prevent them from being discharged both on the ground and into the different water networks or public watercourses.

Will have the safety data sheets of the hazardous products used in the execution of the works, and provide the ENAGÁS representative with a copy of these.

Shall remove and manage all packaging, product residue or impregnated material it owns that is used in the performance of activities in accordance with applicable legislation.

As far as possible, the consumption of water, energy and other related raw materials will be rationalised.

Will maintain the equipment used in the works in a correct state to avoid noise and nuisance to the environment or uncontrolled emissions.

#### Spills

In the event of spillage, the following procedure will be enacted, with constant adherence to the instructions given in the safety sheets for the spilt products:

##### Immediate Action

- Stop the spillage from continuing to occur.
- Use physical means to contain the spilt product.
- In the case of liquids, prevent the spillage from affecting the water networks of the facility or site by directing it towards protective ground cover and without drains or drainage channels.
- If the spill affects the discharge networks, action will be taken with the means available to minimise the effects on the receiving environment and the ENAGÁS representative will be notified immediately.

##### Subsequent Action

- Do not wash the spillage with water.
- Collect the contained product in watertight containers appropriate for the characteristics of the spilt product.
- In the case of liquids, absorb residual liquid with sand, sepiolite or other inert absorbent, or mop up and dispose of in suitable containers.
- Identify the container with respect to the product it contains and manage it as hazardous waste in accordance with current legislation.

## **Waste management**

ENAGÁS facilities and work areas will not accumulate waste in an uncontrolled manner, especially that which may pose a risk to the environment; to this end, the contracted companies will separate and deposit the waste generated by their activities and prevent these from mixing with each other.

Hazardous waste will be deposited separately in appropriately marked containers suitable for the waste in question.

Inert waste from construction and renovation works will be deposited in a separate area for subsequent management.

Separate collection systems are established for waste that can be reused or recycled whenever possible.

The waste will be suitably stored and labelled until the contracted company removes it in accordance with the legislation in force and the execution programme of the works, and it will have to prove to the ENAGÁS representative that these steps have been taken.

In the event of waste materials supplied by ENAGÁS, these will be dealt with in accordance with the ENAGÁS Environmental Procedure "Waste Management", for which instructions should be sought from the ENAGÁS representative.

## **Maintenance of air conditioning systems**

The companies contracted to carry out these activities must provide their accreditation as authorised maintenance companies.

Maintenance work is carried out in accordance with the provisions of the Regulation on Thermal Installations in Buildings, ensuring that no substances are released into the atmosphere and that the products replaced are recovered for recycling or destruction.

## **Environmental controls**

The companies entrusted through contracts with the control of the environmental parameters will attach the relevant calibration certificate to the results report. The submission of this certificate is not required as long as the contracted company is accredited by ENAC to perform the controls that are the subject of the service and the report reflects the uncertainty of the result obtained.

### **• Atmosphere**

The companies contracted to carry out regulatory inspections of combustion sources must record the results in an inspection report containing all the data required by the applicable legislation and enter the results of the inspections in the relevant records or IT equivalent.

These reports will reflect the conclusions regarding compliance with the legal limits.

### **• Noise**

The companies contracted to determine noise emission levels in the vicinity of ENAGÁS facilities will record the results in an inspection report containing the following:

- Description of the methodology used for the measurements, in accordance with the criteria established in the Municipal Ordinance or the corresponding regional regulations. If these regulations do not exist, the company will use its own methodology.
- Indication of the existing legal limit values. If no legal reference exists, the report will reflect this fact.
- Assessment of background noise levels and methodology used.
- Identification of the area where the installation is located and corresponding diagram showing the measurement points.
- If there are legal limits, conclusions on their compliance.

### **• Surplus**

Companies that carry out discharge controls will report the results obtained, comparing each parameter either with the limit values laid down in the relevant discharge authorisation or, in the absence thereof, with the limit values laid down in the applicable legislation. These reports will reflect the conclusions regarding compliance with the legal limits.

## **Energy efficiency**

As far as possible, contracted companies will contribute at all times to the efficient use of available energy sources, to improve competitiveness and reduce greenhouse gas emissions and other related environmental impacts.

They also undertake to comply with current legislation on energy use and consumption and energy efficiency.

#### **Nuisance activities**

No nuisance emissions in excess of the legally permissible emission levels for air quality and the water environment will be generated during the performance of work or the provision of services. Similarly, no noise will be generated that is considered to be a nuisance because it exceeds the applicable legal requirements and no offensive odours will be generated.

#### **Hazardous activities**

Before carrying out any activity involving actual or potential combustion or chemical reaction, or before temporarily storing flammable or corrosive products, the corresponding authorisation must be obtained from ENAGÁS' representative.

All signs and regulations existing at the centre regarding fire prevention, the conduct of the use of energy, the use of machinery, areas where smoking is prohibited or works where there is a risk of fire must be observed.

#### **Emergency situations**

In the event of an environmental emergency, employees of the contracted company will act in accordance with the existing regulations and instructions at the ENAGÁS centre.

In any case, and prior to commencing the execution of the works, the contracted company will consult with the ENAGÁS representative on any doubts regarding these conditions and courses of action.

In addition, contractors and suppliers will at all times seek to apply best practice in environmental and energy efficiency management and identify opportunities for continuous performance improvements within their business activities.

## **1. General cybersecurity clauses**

*This cybersecurity clause applies to all computer and non-computer services that in any way entail access to Enagás' or the Provider's systems and/or the electronic exchange of information.*

The PROVIDER must process ENAGÁS' data with the utmost confidentiality, following the instructions received from the latter regarding the purpose, content, use or processing.

The PROVIDER shall only gain access to ENAGÁS' information in order to fulfil the obligations covered by the Order.

The PROVIDER shall only store permitted data, and it will refrain from storing any information without ENAGÁS' express knowledge and authorisation.

The PROVIDER shall ensure that ENAGÁS' information is not shared with third parties and that no unknown technological resources will be used without ENAGÁS' express authorisation.

The PROVIDER must implement suitable mechanisms to ensure that ENAGÁS' data can only be accessed by users who require them to perform their functions. In doing so, it will provide effective access control and isolation and prevent access between different environments.

The PROVIDER shall constantly guarantee that the tools used in the execution of the Order do not infringe the intellectual property of third parties or any regulations, Orders, rights or property interests of third parties.

The PROVIDER shall always identify the subcontractors involved in the execution of the Order. In turn, it will pass on the technological and safety requirements to the subcontractors and regularly monitor their compliance.

The PROVIDER shall keep the anti-virus protection in the user's systems and equipment employed for the execution of the Order operational and updated at all times.

The PROVIDER shall implement the security controls and mechanisms required to protect the portable and mobile devices and the ENAGÁS media used for the execution of the Order.

In the event that the PROVIDER detects or suspects that a security incident affecting the execution of the Order has occurred, it must immediately inform ENAGÁS' Customer Service Centre by sending an email to [DSI.CAU@enagas.es](mailto:DSI.CAU@enagas.es) or calling 917 099 755.

The PROVIDER shall implement the appropriate information security measures to protect the information related to the execution of the Order.

## 2. Basic cybersecurity requirements

*The following clauses are applicable when the PROVIDER provides any of the following services:*

- *The PROVIDER manages, maintains or implements critical or non-critical systems or applications located at ENAGÁS' facilities.*
- *The PROVIDER provides the service at its own location or facilities or by using its own information systems.*
- *The PROVIDER uses disruptive technologies such as Artificial Intelligence to carry out the Order.*

The PROVIDER must have a security policy that defines and assigns the responsibilities for the technological risk and information security management required to perform the service.

The PROVIDER shall have a technological risk and information security manager. This manager will coordinate with ENAGÁS in security matters and guarantee the completeness, confidentiality and availability of the data and/or systems.

The PROVIDER shall perform regular reviews of the information security and technological risk regulatory framework. By means of the above reviews, the PROVIDER will stay aligned with the business goals and strategies. These reviews will be approved by a manager and give rise to risk mitigation action plans to ensure that the security measures are complied with, effective and updated.

The PROVIDER must conduct a risk analysis of the service provided to ENAGÁS. The analysis shall be conducted on a regular basis and, additionally, when any significant changes in the technological environment occur. The PROVIDER shall monitor the effectiveness of the actions defined for the handling of the risks. The analyses shall be made available to ENAGÁS, which may request them if it deems it appropriate to do so.

The technological risk and security managers appointed by the PROVIDER must collaborate with their counterparts at ENAGÁS and be available at all times for any correspondence, meetings or coordination committees. Monitoring activities may be carried out and the necessary action plans may be defined during the meetings to guarantee the proper performance of the service.

The PROVIDER shall establish a set of rules to ensure acceptable use of ENAGÁS' information and the assets linked to the execution of the Order.

The PROVIDER shall have procedures and mechanisms in place to classify the information in accordance with the legal requirements and the criticality and sensitivity of each kind of information.

The PROVIDER must design a diagram that details the flow of ENAGÁS' data in its systems and/or those of third-party subcontractors.

The PROVIDER shall implement mechanisms to prevent the leakage of information from the devices that process ENAGÁS' information. In the event that the operation requires the output of information from the systems or the devices that store it, both the information and the devices must be encrypted.

The PROVIDER shall ensure that the best practices are applied to ENAGÁS' information and systems, in accordance with the regulatory requirements and information security standards.

The PROVIDER shall assist ENAGÁS in the fulfilment of its inspection, supervision and audit obligations, directly or through:

- a) any regulator with competences in the matter,
- b) ENAGÁS' corporate internal audit unit or any of its local units or departments, and
- c) third-party auditors in the exercise of their responsibilities.

The scope of said obligation will extend to any data, files or assets related to the scope and purpose of the Order. This obligation entails free and unrestricted access for the persons tasked with the inspection or audit to the PROVIDER's facilities, equipment, systems and documents related to the execution of the Order which are relevant to ENAGÁS. The information obtained will be regarded as the PROVIDER's confidential information and it will be treated as such by ENAGÁS.

The audit or inspection may be conducted at any of the PROVIDER's facilities at which information, files or data relating to or resulting from the execution of the Order are kept (regardless of the medium on which they are stored) and, if it is conducted in person, during normal working hours. ENAGÁS will inform the PROVIDER in writing of its intention to conduct any inspection or audit with at least seven (7) days' notice prior to its commencement, indicating its purpose and justification. ENAGÁS will interfere with the PROVIDER's ordinary activity as little as possible during the activity.

The PROVIDER shall not incur any costs or expenses as a result of conducting the regulatory inspections or audits established herein; for these purposes, the following will not be regarded as costs or expenses chargeable to ENAGÁS: (a) the working time devoted by the PROVIDER's personnel to their cooperation with the regulator or the person in charge of the audit, or (b) any related to the supplies at the PROVIDER's facilities in which the regulatory inspection or audit is carried out.

If ENAGÁS uses a third party to conduct the above reviews or audits, the PROVIDER may object to their appointment, if it can be reasonably claimed that said third party has business interests in the PROVIDER's sector. In such a case, ENAGÁS will appoint another third party with proven experience that is not in the above situation. In any event, before starting the verification work, the PROVIDER may require ENAGÁS to sign a confidentiality agreement with said third party under the usual terms for this kind of activity, to the PROVIDER's reasonable satisfaction.

In keeping with the action plans agreed upon by ENAGÁS, once the PROVIDER has been heard, the latter must address any control weaknesses identified in the reviews conducted by ENAGÁS.

The PROVIDER must implement an annual training and awareness-raising programme on best information security practices for its employees, including the right action to be taken in the event of potential cyber incidents during the execution of the Order.

The PROVIDER must ensure that the employees involved in the execution of the Order are aware of the codes of conduct and internal regulations applicable to the correct processing of ENAGÁS' information.

The PROVIDER must have procedures outlining the operation for the execution of the Order. Such procedures will be kept updated and made constantly available to the employees.

The PROVIDER must keep ENAGÁS' information and the systems used for the execution of the Order identified.

The PROVIDER shall implement the necessary integrity controls to prevent any unauthorised modifications of ENAGÁS' information.

The PROVIDER shall have the necessary resources to enable it to dynamically and optimally deal with any fluctuations in the volume of the transactions, ensuring and maintaining the quality of the service within the agreed limits.

The PROVIDER must define a policy for any unauthorised software on user equipment and production systems involved in the execution of the Order.

Before any hiring, the PROVIDER must verify the training and references of the employees and external parties involved in the fulfilment of the purpose of the Order.

The PROVIDER and ENAGÁS shall jointly define the communication protocols for cases of cyber attacks, security incidents and information leakages with a negative impact on ENAGÁS, paying particular attention to the timing and diligence of the actions.

The configuration of the anti-virus protection tools in systems and user equipment employed by the PROVIDER will be restricted to the administrative personnel.

The PROVIDER must establish mechanisms that can dissociate, anonymise, obfuscate or tokenise any of ENAGÁS' information related to the purpose of the Order.

The PROVIDER must comply with the applicable legislation during the processing or storage of ENAGÁS' personal data.

Sensitive information will never be sent by email, but rather through communication gateways between the systems of ENAGÁS and the PROVIDER designed for the purpose.

### **3. Clauses applicable to administration and maintenance services and the implementation or development of systems or applications at ENAGÁS**

*The following clauses, in addition to those contained in points 1 and 2, apply to the services for which the PROVIDER administers, maintains or implements critical or non-critical systems or applications located at ENAGÁS' facilities.*

The PROVIDER shall not use ENAGÁS' actual data for tests or in non-production environments.

The PROVIDER shall implement the security mechanisms required to ensure the proper administration and operation of the security devices.

The PROVIDER must provide ENAGÁS with the requested technical information on the resources to be used, so that compatibility tests can be carried out on applications prior to their implementation. In the event of any substantial modifications (updates, improvements, patches, etc.) of the certifications or security measures applicable to the execution of the Order, the PROVIDER will provide ENAGÁS with the information required to resolve any potential incidents resulting from these modifications.

The PROVIDER shall carry out security reviews of any component of the system used for the execution of the Order in non-production environments.

The PROVIDER must test the software updates and new licences in previous environments before putting them into production.

The PROVIDER shall put controls in place to detect and apply the security updates. It must also test such updates prior to their installation, in order to assess their effectiveness and their potential side effects on the service covered by the Order.

The PROVIDER must have a procedure to manage any changes that may have to be made to the applications or systems involved in the execution of the Order.

The PROVIDER shall establish the appropriate security controls in relation to the acquisition or development of new applications or systems that it intends to use for the execution of the Order.

The PROVIDER must establish a baseline for the security requirements throughout the software development life cycle, with the aim of preventing and addressing any threats and errors in the early stages of the development.

The PROVIDER must apply techniques aligned with best practices to securely develop the software for the applications provided to ENAGÁS.

The PROVIDER must guarantee segmentation between the development, test and production environments for the development of the applications forming part of the scope and purpose of the Order.

The PROVIDER must test the new developments or modifications made to the existing software involved in the execution of the Order before putting them into production.

ENAGÁS may require that any software developments customised for it by the PROVIDER be made available, including the source code, object code, manuals or any other relevant information, whether ENAGÁS owns them under the terms of the Order or otherwise.

The PROVIDER must regularly conduct security analyses/tests on the systems, services, software and other elements that comprise the scope and purpose of the contract. These reviews may be conducted by an independent third party using methodologies accepted by the industry.

The PROVIDER shall perform security hardening tasks on the systems applied to the execution of the Order.

The PROVIDER shall establish the mechanisms required to ensure the protection of all the audit records, guaranteeing the safekeeping and retention of said records for the time established by ENAGÁS, or as determined by the current regulations.

The PROVIDER must monitor the resources used in the execution of the Order, in accordance with the needs of the operation.

The PROVIDER shall perform active monitoring tasks for the prompt management of any alerts, immediately informing ENAGÁS of potential security breaches of the information systems that process ENAGÁS' information.

The PROVIDER shall have monitoring elements that pay special attention to any access to and use of ENAGÁS' identifying information.

The PROVIDER must implement a process for the management of technical vulnerabilities allowing it to identify, document and correct them, so as to mitigate the risk of ENAGÁS' information being exposed.

The PROVIDER shall have a procedure for the management and reporting of security incidents in relation to the services, particularly those affecting ENAGÁS' information. In accordance with the above procedure, the PROVIDER shall collect all the information generated in relation to any incident, from its detection to its resolution, and inform ENAGÁS.

In the event of a security incident associated with the execution of the Order, the time taken by the PROVIDER to act and resolve it will be in accordance with the service availability requirements.

The PROVIDER shall regularly test the incident response plan and implement the changes required for the continuous improvement of the entire process. The results report must be made available to ENAGÁS should it request it.

The PROVIDER must have a regulatory framework to control the logical access to the systems which is aligned with ENAGÁS' service requirements.

The PROVIDER shall implement a formalised process for registering users in the systems that clearly defines the circuit for the provisioning, profiling and de-provisioning of the users involved in the execution of the Order. The profiling shall ensure that the users have access to the minimum information required to perform their work.

The PROVIDER shall establish the necessary and sufficient security measures to ensure that the administrators' access to the information systems linked to the service is implemented using encrypted channels and strong authentication.

The PROVIDER shall have a procedure to ensure regular reviews of the access permissions and access controls configured in the systems involved in the execution of the Order.

The PROVIDER shall implement mechanisms for the immediate processing of the user de-registrations, guaranteeing the removal of all kinds of access by the de-registered user.

The PROVIDER must establish a password management procedure for the systems used in the execution of the Order, requiring, among other measures, changing the initial password, an appropriate length and level of complexity for passwords to minimise the risk, a definition of the password expiry dates and a number of records that prevent reuse.

In its password policies associated with the execution of the Order, the PROVIDER must include a password management procedure to ensure that they are only known by the user.

The PROVIDER's information processing systems must guarantee the encrypted storage of the passwords associated with the development of the purpose of the Order.

The PROVIDER must always be able to identify the external and internal users who have access to the information provided by ENAGÁS for the execution of the Order.

The PROVIDER must establish sufficient and necessary measures to ensure that access to the administration tools of the systems related to the purpose of the Order is strictly reserved to personnel with the above roles and responsibilities.

The PROVIDER must maintain protection measures for the files, equipment and systems involved in the implementation of the Order based on the international standards.

The PROVIDER must record all the activity of the events related to the users involved in the execution of the Order. Said activity will consist of the logs of all the systems directly or indirectly involved in the execution of the Order, including those relating to intermediate temporary storage systems. The format and content of these logs shall include all the information that allows for proper traceability of the events. The availability of the logs shall be established for a fixed period of real time, or, by default, by means of transfer or access to the internal repositories.

The PROVIDER must have a business continuity plan to guarantee the provision of the service should a disruptive event occur.

The PROVIDER's business continuity plan shall be aligned with the needs of the service, and it shall cover both the procedures and the times admissible for the recovery of the systems and the service continuity.

The PROVIDER must regularly test the business continuity plan and analyse the results of the tests that are conducted in order to apply them to the corrective and improvement plans.

The PROVIDER shall implement mechanisms to prevent denial-of-service attacks hindering the normal provision of the service.

The PROVIDER shall employ procedures to generate backup copies and recover information that encompass the data, the system configurations, etc. The copies must be hosted in locations other than those that support the usual operation of the service.

The PROVIDER shall regularly make backup copies of the systems involved in the execution of the Order, depending on the criticality of the services provided, in order to guarantee the full recovery of the systems in the event of an incident.

The PROVIDER shall implement the logical and physical security measures required to ensure the completeness, confidentiality and availability of the backup copies of the information in the systems involved in the execution of the Order throughout the chain of custody.

The PROVIDER shall take out and maintain in force during the course of the Order, at its own expense, the following insurance policy: A Cybersecurity Policy, with Civil Liability cover in the event of an information security incident or a breach of privacy, regarded as a breach of the system, unauthorised access to the data contained in ENAGÁS' computer system and Liability with regard to digital media as a result of an act, error or omission resulting from any reproduction, publication, announcement of information or digital content by the PROVIDER on its websites and/or its profiles on social media that involves defamation, slander, infringement of the right to honour or damage to the reputation of a natural or legal person, a breach of any intellectual property right, copyright, slogan, brand, company name, licence, information or domain name, or a breach of the right to privacy or image rights, or theft or identity theft. This Policy must include an indemnity limit with a minimum €1 million cover.

#### **4. Clauses applicable to services in the cloud, with internet access or located outside ENAGÁS**

*The following clauses, in addition to those contained in points 1 and 2, apply to services for which the PROVIDER performs the service at its own location or facilities or by using its own information systems.*

When ENAGÁS' information is stored in the PROVIDER's systems, the latter must guarantee the option of encryption in accordance with ENAGÁS' information classification policy. The PROVIDER shall only use strong encryption algorithms.

The PROVIDER shall at all times guarantee the legal, statutory and regulatory compliance applicable to the security of ENAGÁS' information, at all the locations and infrastructures in which its information is stored and processed.

The PROVIDER shall provide ENAGÁS with the human and material resources required to analyse and remediate incidents. This will enable ENAGÁS to analyse and investigate the logs of the systems, traces of the IDS elements, firewall and any network and security elements deployed at the PROVIDER's facilities. For this purpose, the PROVIDER shall retain the logs and traces for at least seven (7) days following the date of reporting of the incident, and it shall preserve and isolate any electronic evidence or any other kind of evidence that may be useful for forensic analysis, should it be necessary.

The PROVIDER of the SaaS (Software as a Service) service must have an SLA (Service Level Agreement) for the availability of the service to be provided.

The PROVIDER of the SaaS service must have a monitoring model to comply with the availability SLA.

The PROVIDER of the SaaS service must have a procedure for applying penalties for non-compliance with the availability SLA.

The PROVIDER of the SaaS service must have a procedure or schedule indicating the times the service will be unavailable during the performance of maintenance tasks.

The PROVIDER of the SaaS service must have a communication procedure to announce any change or evolution of the service that may affect ENAGÁS.

The PROVIDER of the SaaS service must specify where its service is hosted, be it in public cloud infrastructure, in the manufacturer's own private cloud infrastructure or in hybrid (public and private) cloud infrastructure.

When the infrastructure it uses is in the public cloud, the PROVIDER of the SaaS service must indicate which CSP (Cloud Service Provider) is hosting it.

The PROVIDER of the SaaS service must ensure that the region of deployment of its service for ENAGÁS' use is located in the European Economic Area.

If the SaaS contains sensitive information for ENAGÁS, the PROVIDER must ensure compliance with all the clauses concerning the processing of ENAGÁS' confidential information.

The PROVIDER of the SaaS service must have mechanisms in place to integrate its service by means of SSO access or integration with AD. If the above is not possible, it must ensure that it has some kind of multi-factor authentication (MFA) mechanism for access to its service.

The PROVIDER of the SaaS service must enable a technical support communication channel, as well as a direct contact person to activate it.

The PROVIDER must apply mechanisms for the management of authentication credentials that are aligned with the classification of ENAGÁS' information, in order to ensure its confidentiality and completeness.

The PROVIDER must define and agree with ENAGÁS upon a procedure for the return and transition of the information in the Order that establishes, at least, safeguarding of the logs, revocation of accesses, secure and permanent deletion of ENAGÁS' proprietary information and the delivery and return of ENAGÁS' proprietary assets.

The PROVIDER must provide mechanisms for the portability of the systems or information that help ENAGÁS to incorporate the data into its systems, thus ensuring their completeness and validating their proper transition.

The PROVIDER shall implement the physical security measures required to protect the information systems located outside ENAGÁS' facilities from physical damage or unauthorised access to the information associated with the execution of the Order.

The PROVIDER shall perform maintenance tasks on the technological infrastructure deployed in the execution of the Order, with the aim of preventing possible damage or failures thereof.

The PROVIDER shall implement procedures to manage the removal of media containing sensitive ENAGÁS data from its facilities.

The PROVIDER must guarantee the use of mechanisms to destroy or recycle media and securely eliminate ENAGÁS' information.

The PROVIDER must establish adequate security measures in the event that it stores sensitive ENAGÁS information in physical format. These measures will ensure that the information is afforded a level of protection equivalent to the digital format.

The PROVIDER shall implement the mechanisms required to guarantee the confidentiality, completeness and availability of the information during communication between its infrastructure and that of ENAGÁS, adjusting them to the needs of the service.

The PROVIDER's technological infrastructure whose use is shared with other customers will have measures allowing the logical separation of the information related to the execution of the Order.

The PROVIDER shall ensure that the internal IT environments and those shared with the PROVIDER's other customers are sufficiently isolated and segmented to prevent the spread of a cyber attack suffered by another of the PROVIDER's customers to ENAGÁS' information .

The PROVIDER's network involved in the execution of the Order will be suitably segmented to ensure that users only have access to the resources necessary for the performance of their functions.

The PROVIDER's server that hosts ENAGÁS' database must be installed in a different system from the one running the application.

Communication with the PROVIDER's server in which ENAGÁS' database is hosted must be protected by a logical perimeter security mechanism (a firewall) to restrict direct access via the Internet.

The PROVIDER shall establish the encryption of communications that are made on public and/or private networks, via which information related to the service travels, particularly in the case of confidential data or data subject to regulations.

The PROVIDER shall implement authentication mechanisms to guarantee unequivocal communication with ENAGÁS.

The PROVIDER must segment its organisation's networks and maintain the necessary security levels in each of the network's segments.

The PROVIDER shall have a complete map of the network applied to the execution of the Order. The network map must be made available to ENAGÁS whenever it requests it.

The PROVIDER must establish mechanisms to ensure the control and monitoring of remote accesses to the technological environment assigned to the execution of the Order.

The PROVIDER shall provide ENAGÁS with details of the technical perimeter security measures used to protect the information related to the purpose of the Order.

## 5. Clauses applicable to services that use Artificial Intelligence

*The following clauses, in addition to those contained in points 1 and 2, apply to services for which the PROVIDER, for the execution of the Order, uses disruptive technologies such as Artificial Intelligence.*

The PROVIDER must at all times guarantee compliance with Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules in the field of artificial intelligence, and with all the legislation applicable Artificial Intelligence, data protection and privacy.

The PROVIDER must duly justify the need to use Artificial Intelligence for the intended purposes or goals, avoiding the assumption of unjustified risks of damage.

The PROVIDER must have a model for data management and use of Artificial Intelligence, ensuring transparency throughout all the phases of the data management, including the collection, storage, processing and use.

The Artificial Intelligence systems must treat all people fairly and equally. The PROVIDER must prevent biases in the collection and handling of the data and in the training of the Artificial Intelligence algorithms and tools, avoiding the reproduction of any existing biases and social inequalities.

The PROVIDER must objectively verify the results and functioning of the Artificial Intelligence by means of regular audit procedures and allow independent audits.

The Artificial Intelligence systems must allow individuals to know when they are interacting with them, informing them of the rights protecting them and giving them the opportunity to object to the results of said interaction and request human intervention, including in the area of automated individual decisions and profiling, as provided for in Regulation (EU) 2016/679.

The PROVIDER must record the algorithms that use Artificial Intelligence, expressly indicating their purpose(s). These records will be made available in a transparent and accessible manner at the request of the competent authority.

The PROVIDER must have mechanisms in place to react to any incidents that occur during the management of the system and the operational procedures that depend on it.

It must provide detailed documentation on the functioning of the Artificial Intelligence system, including the algorithms that are used, the training data and the decision-making processes. The Artificial Intelligence system must be able to explain its decisions in a manner understandable to humans.

The data that are used must be protected in accordance with the applicable laws, including Regulation (EU) 2016/679. Special category data must be anonymised to prevent the identification of individuals.

It must implement robust cybersecurity measures to protect the data from unauthorised access, theft and manipulation.

The Artificial Intelligence system must undergo performance tests to guarantee its efficiency and effectiveness in different operational scenarios. It must implement continuous monitoring systems to detect and remedy errors and failures in real time.

The PROVIDER must undertake to continuously maintain and improve the Artificial Intelligence system, incorporating new technologies and improvements based on user feedback and advances in the field of Artificial Intelligence.

It must provide suitable training for users on the use and restrictions of the Artificial Intelligence system and offer ongoing technical support to resolve any problems that may occur.

The PROVIDER must assume responsibility for any malfunction or damage caused by the Artificial Intelligence system and establish clear mechanisms for repairing any damage or harm that is caused.

The PROVIDER must, in accordance with the service's degree of risk, comply with the following clauses:

- **Minimal Risk Artificial Intelligence:** guarantee basic compliance with the data protection and privacy standards.
- **Moderate Risk Artificial Intelligence:** implement robust security measures and ensure that the Artificial Intelligence systems can be audited.
- **High Risk Artificial Intelligence:** demonstrate compliance with a broader set of rules and regulations, including impact assessments and risk mitigation measures.
- **Critical Risk Artificial Intelligence:** comply with the highest standards and be subject to highly rigorous oversight, including the need for independent certification and contingency measures for emergency situations.

## **Data processing clauses**

*The following clauses will apply to services for which the PROVIDER accesses personal data belonging to ENAGÁS.*

### **1. Purpose and duration**

Owing to the activity it provides for ENAGÁS, the PROVIDER may gain access to personal data belonging to the former.

For these purposes, ENAGÁS will be regarded as the data controller (hereinafter, the Data Controller) and the PROVIDER will be regarded as the data processor (hereinafter, the Data Processor), in accordance with the provisions of Chapter V of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights, and pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 (hereinafter, the GDPR).

- Purpose of the processing

The data processing is performed within the framework of the provision of a service covered by this Order.

In the course of the provision of the service, the PROVIDER may access and process certain personal data belonging to ENAGÁS, in its status as Data Processor.

These clauses authorise the PROVIDER (or the Data Processor) to process the personal data required to provide the above-mentioned service on behalf of ENAGÁS (or the Data Controller) under its instructions.

- Duration of the processing

The processing of the personal data covered by this Order will continue throughout the term of the contract. Any amendment to this clause must be made in writing and signed by the legitimate representatives of each of the Parties with sufficient power.

### **2. Description of the processing and information concerned**

In order to fulfil the purpose of the indicated services, the processing, depending on the service provided, may consist of the following operations: collection, organisation, modification, interconnection, deletion, adaptation, communication, comparison, destruction, structuring, use, extraction, dissemination, restriction, display, approval, storage, blocking, registration or consultation.

Moreover, the categories of data subjects covered by the processing may, as appropriate, be: employees, applicants, directors, senior officials, contractors, external people who visit the facilities, members of the board or shareholders.

The personal data will only be processed for justified reasons in accordance with the confidentiality and secrecy requirements, respecting the rights and obligations of each of the parties.

### **3. The Parties' obligations**

Both parties undertake to comply with the provisions of the above-mentioned data protection regulations.

A) The PROVIDER's obligations

The PROVIDER, as the Data Processor, undertakes to process the data in keeping with ENAGÁS' instructions and in accordance with the following obligations:

- Restriction of the purpose of the processing

It will only access the personal data when they are essential for the proper performance of the services for which it has been contracted, without assigning, applying or using the data for purposes other than those indicated in this Order or in any other way that would entail a breach of the instructions of the Data Controller.

In the event that it uses the data for a different purpose, discloses them or uses them in breach of the Order or the obligations of the current regulations, the Data Processor will assume the status of Data Controller and will be held liable for any infringements that are committed.

- Duty of secrecy and confidentiality

The Data Processor undertakes to maintain the utmost confidentiality and secrecy with regard to the personal data to which it has access by virtue of the processing, even after the purpose of the service has come to an end. In any event, the people authorised to process the Personal Data will undertake to respect the obligation of confidentiality and comply with the obligations relating to the processing of personal data.

The Data Processor will not allow the personal data to be accessed by its personnel, partners and all the people under its responsibility who do not have a need to know them in order to provide the contracted services.

- Disclosure to third parties

It will not reveal, transfer, assign or otherwise disclose the personal data, either verbally or in writing, by electronic means, on paper or by means of computer access, to any third party, not even for their storage, without a prior authorisation or instruction from the Data Controller.

- Record of Processing Activities

In the event that it is obliged to record the processing activities, the Data Processor will keep a record of all the categories of processing activities carried out on behalf of the Data Controller that contains the information required by the regulations.

- Oversight

It will provide the Data Controller with all the information required to demonstrate compliance with the obligations set out in article 28 of the GDPR, as well as for the audits or inspections conducted by the Data Controller or any other auditor authorised by the latter.

- Training

It will guarantee the necessary training in personal data protection for the people authorised to process the personal data.

- Data Protection Officer

If it is obliged to do so by article 37.1 of the GDPR, it must appoint a data protection officer and communicate his/her identity and contact details to the Data Controller, in compliance with all the provisions of articles 37, 38 and 39 of the GDPR for the processing of the personal data.

- Security measures

The Data Processor must implement and adopt the appropriate technical and organisational measures to ensure a degree of security appropriate to the risk, in such a way that they prevent the data's destruction, alteration, loss or unauthorised disclosure or access, in accordance with article 32 of the GDPR.

In particular, the parties must: (i) Guarantee the constant confidentiality, completeness, availability and resilience of the processing systems and services; (ii) Restore the availability of and access to the personal data promptly in the event of a physical or technical incident; (iii) Regularly verify, evaluate and assess the effectiveness of the technical and organisational measures implemented to guarantee the security of the processing and; (iv) Pseudonymise and encrypt the personal data, if necessary.

Among others, it must carry out the following measures:

- a. Control any access to the systems via which the PROVIDER may gain access to personal data by means of the establishment of identification and authentication measures.
- b. Draw up policies, standards and procedures for the secure management of any kinds of media that store personal data and allow their transfer from the main data processing locations.
- c. Make regular backup copies and perform regular recoveries.
- d. Define the roles and obligations of each of the users or user profiles that may have access to the data and information systems.
- e. Carry out training initiatives on understanding these duties and the consequences of failure to comply with them.
- f. Report and record any security incidents that may pose a risk to the confidentiality or completeness of the data, and report any breaches of the security of the personal data, in accordance with the procedures that have been established.

- Assistance for the Data Controller
 

It will support the Data Controller, for a reasonable period of time determined by the Data Controller, within the maximum limits established by the GDPR, in order to comply with the obligations defined in the following articles:

  - i. article 32 of the GDPR (Security of the processing);
  - ii. articles 33 and 34 of the GDPR (Reporting a personal data security breach);
  - iii. article 35 of the GDPR (Data protection impact assessment, as appropriate) and
  - iv. article 36 of the GDPR (Prior consultation of the supervisory authority).
- Exercise of rights
 

The Data Processor shall notify the Data Controller of any request to exercise the rights of access, rectification, erasure, objection, restriction of the processing or data portability or the right not to be subject to automated individualised decisions, made by any data subject whose data have been processed by the Data Processor in order to fulfil the purpose of this Order, when such rights are applicable, so that the Data Controller may resolve the request before the deadline established in the current regulations.

The request must be sent to the Data Controller as quickly as possible, together with, as appropriate, any other information that may be relevant to the resolution of the request.

Requests should be sent in writing to Paseo de los Olmos nº 19, 28005 Madrid with a reference to "Data Protection", enclosing a photocopy of an ID card, or by sending an email to [protecciondedatos@enagas.es](mailto:protecciondedatos@enagas.es).
- Reporting data security breaches
 

The Data Processor will inform the Data Controller without any undue delay and, in any event, within 72 hours, in a reasoned manner, of any breaches of the security of the personal data under its responsibility of which it becomes aware, together with all the relevant information for the documentation and reporting of the incident.

If it is available, the following information will at least be provided, together with all the relevant information for the documentation and reporting of the incident:

  - a. A description of the nature of the personal data security breach, including, whenever possible, the categories and the approximate number of data subjects affected and the categories and approximate number of personal data records affected.
  - b. The person's contact details to obtain further information.
  - c. A description of the potential consequences of the personal data security breach. A description of the measures taken or proposed to remedy the personal data security breach, including, as appropriate, the measures taken to mitigate any potential negative effects.

A notification will not be required when such a security breach is unlikely to constitute a risk to the rights and freedoms of natural persons.

If and inasmuch as it is not possible to provide the information simultaneously, it will be gradually provided without any undue delay.
- Outsourcing
 

In the event that all or part of the services covered by this Order involving the processing of personal data is outsourced, the Data Processor will inform the Data Controller in writing with sufficient notice, indicating the processing operations to be outsourced and clearly and unequivocally identifying the subcontracting company and its contact details.

The subprocessor, which will also have the status of processor, will also be obliged to comply with the obligations established in this Order for the Data Processing, as well as the instructions issued by the Data Controller.
- Transfers of data to third [i.e. non-EU] countries
 

The Data Processor may only transfer personal data to a third country or international organisation if it has offered adequate safeguards in accordance with article 46 of the GDPR, provided that the data subjects have enforceable rights and effective legal actions.

- Destination of the data upon the completion of the contractual relationship

Once the Order has been completed, the Data Processor undertakes to return, forward to another provider or fully delete the personal data (or medium or document containing them), at the choice of the Data Controller, provided that there is no legal provision requiring them to be kept, in which case they may not be destroyed.

However, the Data Controller authorises the Data Processor to retain a copy of the personal data duly and technically blocked for as long as liabilities resulting from the provision of the services covered by the Order may arise.

B) ENAGÁS' obligations

ENAGÁS, as the Data Controller, undertakes to:

- a) Deliver to the Data Processor the data to be processed as indicated in this Order and the necessary documentation.
- b) Issue the instructions to the Processor regarding the processing of data that it deems necessary. The instructions will be deemed to include, among others, as appropriate, any obligations binding the Data Processor provided for in this Order.
- c) Respond to notifications received from the Data Processor regarding the processing of the data, in particular, any relating to outsourcing of the processing, security breaches and instructions issued by the Data Controller which, in the Data Processor's opinion, infringe the data protection regulations.

In this regard, the Data Controller will notify the supervisory authority in the event of a personal data security breach within a maximum of 72 hours.

- d) Ensure, prior to and throughout the processing, compliance with the data protection regulations, guaranteeing that the processing requested from the Data Processor complies with said regulations.
- e) Supervise the processing of the data.

## **Clauses on the processing of data by ENAGÁS on behalf of a third party**

*The following clauses will apply to services for which ENAGÁS accesses personal data whose processing is performed by the CUSTOMER.*

### **1. Purpose and duration**

Owing to the activity it provides for the CUSTOMER, ENAGÁS may gain access to personal data that belongs to it.

For these purposes, the CUSTOMER will be regarded as the data controller (hereinafter, the Data Controller) and ENAGÁS will be regarded as the data processor (hereinafter, the Data Processor), in accordance with the provisions of Chapter V of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights, and pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 (hereinafter, the GDPR).

- Purpose of the processing

The data processing is performed within the framework of the provision of a service covered by this Order.

In the course of the service provision, ENAGÁS may access and process certain personal data belonging to ENAGÁS, in its status as Data Processor.

These clauses authorise ENAGÁS (or the Data Processor) to process the personal data required to provide the above-mentioned service on behalf of ENAGÁS (or the Data Controller) under its instructions.

- Duration of the processing

The processing of the personal data covered by this Order will continue throughout the term of the contract. Any amendment to this clause must be made in writing and signed by the legitimate representatives of each of the Parties with sufficient power.

### **2. Description of the processing and information concerned**

In order to fulfil the purpose of the indicated services, the processing, depending on the service provided, may consist of the following operations: collection, organisation, modification, interconnection, deletion, adaptation, communication, comparison, destruction, structuring, use, extraction, dissemination, restriction, display, approval, storage, blocking, registration or consultation.

Moreover, the categories of data subjects covered by the processing may, as appropriate, be: employees, applicants, directors, senior officials, contractors, external people who visit the facilities, members of the board or shareholders.

The personal data will only be processed for justified reasons in accordance with the confidentiality and secrecy requirements, respecting the rights and obligations of each of the parties.

### **3. The Parties' obligations**

Both parties undertake to comply with the provisions of the above-mentioned data protection regulations.

#### A) ENAGÁS' obligations

ENAGÁS, as the Data Processor, undertakes to process the data in keeping with ENAGÁS' instructions and in accordance with the following obligations:

- Restriction of the purpose of the processing

It will only access the personal data when they are essential for the proper performance of the services for which it has been contracted, without assigning, applying or using the data for purposes other than those indicated in this Order or in any other way that would entail a breach of the instructions of the Data Controller.

In the event that it uses the data for a different purpose, discloses them or uses them in breach of the Order or the obligations of the current regulations, the Data Processor will assume the status of Data Controller and will be held liable for any infringements that are committed.

- Duty of secrecy and confidentiality

The Data Processor undertakes to maintain the utmost confidentiality and secrecy with regard to the personal data to which it has access by virtue of the processing, even after the purpose of the service has come to an end. In any event, the people authorised to process the Personal Data will undertake to respect the obligation of confidentiality and comply with the obligations relating to the processing of personal data.

The Data Processor will not allow the personal data to be accessed by its personnel, partners and all the people under its responsibility who do not have a need to know them in order to provide the contracted services.

- Disclosure to third parties

It will not reveal, transfer, assign or otherwise disclose the personal data, either verbally or in writing, by electronic means, on paper or by means of computer access, to any third party, not even for their storage, without a prior authorisation or instruction from the Data Controller.

- Record of Processing Activities

In the event that it is obliged to record the processing activities, the Data Processor will keep a record of all the categories of processing activities carried out on behalf of the Data Controller that contains the information required by the regulations.

- Oversight

It will provide the Data Controller with all the information required to demonstrate compliance with the obligations set out in article 28 of the GDPR, as well as for the audits or inspections conducted by the Data Controller or any other auditor authorised by the latter.

- Training

It will guarantee the necessary training in personal data protection for the people authorised to process the personal data.

- Data Protection Officer

If it is obliged to do so by article 37.1 of the GDPR, it must appoint a data protection officer and disclose his/her identity and contact details to the Data Controller, in compliance with all the provisions of articles 37, 38 and 39 of the GDPR for the processing of the personal data.

- Security measures

The Data Processor must implement and adopt the appropriate technical and organisational measures to ensure a degree of security appropriate to the risk, in such a way that they prevent the data's destruction, alteration, loss or unauthorised disclosure or access, in accordance with article 32 of the GDPR.

In particular, the parties must: (i) Guarantee the constant confidentiality, completeness, availability and resilience of the processing systems and services; (ii) Restore the availability of and access to the personal data promptly in the event of a physical or technical incident; (iii) Regularly verify, evaluate and assess the effectiveness of the technical and organisational measures implemented to guarantee the security of the processing and; (iv) Pseudonymise and encrypt the personal data, if necessary.

Among others, it must carry out the following measures:

- a. Control any access to the systems via which ENAGÁS may gain access to personal data by means of the establishment of identification and authentication measures.
- b. Draw up policies, standards and procedures for the secure management of any kinds of media that store personal data and allow their transfer from the main data processing locations.
- c. Make regular backup copies and perform regular recoveries.
- d. Define the roles and obligations of each of the users or user profiles that may have access to the data and information systems.
- e. Carry out training initiatives on understanding these duties and the consequences of failure to comply with them.
- f. Report and record any security incidents that may pose a risk to the confidentiality or completeness of the data, and report any breaches of the security of the personal data, in accordance with the procedures that have been established.

- Assistance for the Data Controller

It will support the Data Controller, for a reasonable period of time determined by the Data Controller, within the maximum limits established by the GDPR, in order to comply with the obligations defined in the following articles:

- i. article 32 of the GDPR (Security of the processing);
- ii. articles 33 and 34 of the GDPR (Reporting a personal data security breach);
- iii. article 35 of the GDPR (Data protection impact assessment, as appropriate) and
- iv. article 36 of the GDPR (Prior consultation of the supervisory authority).

- Exercise of rights

The Data Processor shall notify the Data Controller of any request to exercise the rights of access, rectification, erasure, objection, restriction of the processing or data portability or the right not to be subject to automated individualised decisions, made by any data subject whose data have been processed by the Data Processor in order to fulfil the purpose of this Order, when such rights are applicable, so that the Data Controller may resolve the request before the deadline established in the current regulations.

The request must be sent to the Data Controller as quickly as possible, together with, as appropriate, any other information that may be relevant to the resolution of the request.

Requests should be sent in writing to Paseo de los Olmos nº 19, 28005 Madrid with a reference to "Data Protection", enclosing a photocopy of an ID card, or by sending an email to [protecciondedatos@enagas.es](mailto:protecciondedatos@enagas.es).

- Reporting data security breaches

The Data Processor shall inform the Data Controller without any undue delay and, in any event, within 72 hours, in a reasoned manner, of any breaches of the security of the personal data under his/her responsibility of which he/she becomes aware, together with all the relevant information for the documentation and reporting of the incident.

If it is available, the following information will at least be provided, together with all the relevant information for the documentation and reporting of the incident:

- a. A description of the nature of the personal data security breach, including, whenever possible, the categories and the approximate number of data subjects affected and the categories and approximate number of personal data records affected.
- b. The person's contact details to obtain further information.
- c. A description of the potential consequences of the personal data security breach. A description of the measures taken or proposed to remedy the personal data security breach, including, as appropriate, the measures taken to mitigate any potential negative effects.

A notification will not be required when such a security breach is unlikely to constitute a risk to the rights and freedoms of natural persons.

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

- Outsourcing

In general, the Data Controller authorises the Data Processor to outsource the services with access to personal data for which it is the Controller, in accordance with the provisions of this Order.

The authorisation, which covers the entirety of the services provided, will encompass any substitution made due to the needs of the service. Consequently, an objection to the outsourcing of the service made by the Data Controller will give rise to its withdrawal and the cessation of the service.

The subcontractors, which will also have the status of Data Subprocessors, will also be obliged to comply with the obligations established in this Order for the Data Processing, as well as the instructions issued by the Data Controller.

- Transfers of data to third [i.e. non-EU] countries

The Data Processor may only transfer personal data to a third [i.e. non-EU] country or international organisation with the safeguards provided for in article 45 et seq of the GDPR, provided that the data subjects have enforceable rights and effective legal actions.

- Destination of the data upon the completion of the contractual relationship

Once the Order has been completed, the Data Processor undertakes to return, forward to another provider or fully delete the personal data (or medium or document containing them), at the choice of the Data Controller, provided that there is no legal provision requiring them to be kept, in which case they may not be destroyed.

However, the Data Controller authorises the Data Processor to retain a copy of the personal data duly and technically blocked for as long as liabilities resulting from the provision of the services covered by the Order may arise.

#### B) ENAGÁS' obligations

The CUSTOMER, as the Data Controller, undertakes to:

- a) Deliver to the Data Processor the data to be processed as indicated in this Order and the necessary documentation.
- b) Issue the instructions to the Processor regarding the processing of data that it deems necessary. The instructions will be deemed to include, among others, as appropriate, any obligations binding the Data Processor provided for in this Order.
- c) Respond to notifications received from the Data Processor regarding the processing of the data, in particular, any relating to outsourcing of the processing, security breaches and instructions issued by the Data Controller which, in the Data Processor's opinion, infringe the data protection regulations.

In this regard, the Data Controller will notify the supervisory authority in the event of a personal data security breach within a maximum of 72 hours.

- d) Ensure, prior to and throughout the processing, compliance with the data protection regulations, guaranteeing that the processing requested from the Data Processor complies with said regulations.
- e) Supervise the processing of the data.

## **Clauses for data assignments between ENAGÁS and a third party**

*The following clauses will apply in cases in which the Data Controller assigns data to a new Controller that will process the data for its own purposes, in accordance with the provisions of the Order.*

Both parties undertake to guarantee the protection and confidentiality of the personal data received from each other in fulfilment of this Order. This obligation stems from Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD), and Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 (hereinafter, GDPR).

Each of the parties shall independently determine the purposes and means of the processing in relation to the processing operations for which they are responsible.

### **The parties' obligations**

Prior to the disclosure of the data subjects' data, the ASSIGNOR will inform the data subjects of the processing of their data and ensure compliance with the principle of lawfulness of the processing, obtaining, as appropriate, the prior consent of the data subjects.

As for the ASSIGNEE, it undertakes to inform the data subjects, and to apply all the relevant technical and organisational measures to the processing to guarantee their security, under the terms indicated in Regulation (EU) 2016/679, and not to assign the data to third parties or to use such information for purposes other than those indicated in this Order, including the sending of electronic correspondence of a commercial or promotional nature.