PROSEGUR

3P Support Document to General Conditions of Purchase

RESOURCES MANAGEMENT AREA - PURCHASING

1. Owner

Corporate Resource Management Director

2. Scope

Regulatory framework that governs the terms and conditions applicable to any type of contract or order from Prosegur in the absence of specific terms agreed upon by the parties and embodied in the contract.

3. Preparation and Approval

Drafted by:	Resources Management Area - Purchasing				
Revised by:	Legal Area				
Approved by:	Purchasing Area	David Jose Gestal		Date:	23/06/2023
Replacing:	DS/GLO/GdM/COM/01 DS/GLO/GdM/COM/06	Version:	03 02	Date:	03/31/2023 05/31/2022

4. Related Documents

Code	Name
NG/GLO/GdM/COM/01	General 3P PCS Purchase Policy

5. DEFINITIONS

For greater clarity and understanding of these General Terms and Conditions, the following definitions are set forth:

- Prosegur: The company of the Group that acts as buyer and/or contracting party in any purchase and/or contract.

- Subsidiary means the entity or set of entities, whether registered or not, under common control. As used in this definition, “control” (and the variants used) shall mean the power, directly or indirectly, to direct the interests of another entity whether by ownership, contract, or otherwise.

- Purchase: Transaction in which the amount corresponds mainly to acquisitions of goods.

- Procurement: Transaction in which the majority amount corresponds to the acquisition of works and/or services and, consequently, the contribution of labor. Both a purchase and procurement may have components of works, goods and services. In the development of these Terms and Conditions the terms of purchase and procurement shall be considered equivalent terms.

- Order: Document of a binding nature for the parties issued by Prosegur to the supplier, which includes prices, terms and conditions for the supply of a good or provision of a service, to which the purchase or contracting has been previously awarded. Sometimes this document is both a contract and a procurement request.

- Contract: Binding agreement signed between the parties where prices, terms and conditions for the performance of a work, subcontracting of the same or provision of a service are fixed.

- General Terms and Conditions This document establishes the bases for the process of purchasing goods and/or contracting works and/or services and is applicable to the entire Prosegur Group.

- Supplier: The entity that has been awarded an Order.

- Contractor: The entity that has been awarded a Contract.

- Special Terms and Conditions: Also called Request for Proposal. Any document that includes all those requirements, of whatever nature, necessary for the Supplier/Contractor to supply the goods or perform the works and services in the required form and quality.

6. GENERAL TERMS AND CONDITIONS OF PURCHASE AND PROCUREMENT

6.1. Validity and priority of the contractual documentation

6.1.1. The General Terms and Conditions shall be brought to the attention of the Suppliers/Contractors as part of the purchase/contract execution and shall integrate the contractual documentation set forth in the purchase order/contract in all its terms.

6.1.2. These General Terms and Conditions may be supplemented by Special Terms and Conditions and/or the relevant purchase orders/contracts. In case of discrepancies between the documents integrating a purchase/procurement, the Special Terms and Conditions shall prevail over the General Terms and Conditions, in the following order:

- The possible modifications to the Order / Contract, expressly agreed in writing and subsequent to its date of subscription or issuance.
- The Order / Contract and its attached documentation.
- The possible modifications to the requested technical specifications
- The requested technical specifications.
- Modifications to the Special and/or General Terms and Conditions.
- The Special Terms and Conditions.
- General Terms and Conditions
- Clarifications made in writing by the Supplier/Contractor, subsequent to its offer and accepted by Prosegur.

6.1.3. The Supplier's/Contractor's General Terms and Conditions other than those set forth herein shall not be accepted unless expressly accepted by Prosegur in whole or in part.

6.1.4. The conditions and specifications inserted by the Supplier/Contractor in its delivery bills, invoices or other documents crossed between the parties, which are contrary to the express conditions established in the Order/Contract, shall be null and void.

6.1.5. The Contracts for works and/or services shall remain in force for the duration of the execution of the works that are the subject of the contracts, in accordance with the provisions of the contract documents. If an expiration date has been predetermined and the duration of said works exceeds this date, the Contract shall be tacitly extended for successive monthly periods, unless either party announces that it wishes to terminate the Contract in writing at least fifteen days prior to said expiration date or any of the extensions.

However, the Contract may include the clauses that shall be applicable to compliance with performance deadlines and extensions thereof.

6.2. Supplier evaluation and approval system

6.2.1. Prosegur uses an online platform managed by a supplier external to Prosegur (GoSupply Advanced Applications, S.L., hereinafter “GoSupply”) for the pre-classification, evaluation and preliminary approval of its Suppliers/Contractors. For the classification and final approval of a Supplier/Contractor, the registration and participation of the Supplier/Contractor in the Supplier risk analysis process implemented by Prosegur via this platform is a mandatory requirement.

6.2.2. The Supplier/Contractor shall be qualified as eligible in Prosegur’s testing process prior to the commencement of any supply of services, goods and/or materials under these General Terms and Conditions and/or the relevant Contract/Order. In addition, the Supplier/Contractor guarantees and undertakes to maintain the conditions approved in the aforementioned analysis throughout the term of these General Terms and Conditions and/or the relevant Contract/Order III and to this end, undertakes to provide Prosegur with the requested information and/or updated documentation in accordance with the criteria established by Prosegur.

6.2.3. The Supplier/Contractor is informed and accepts that Prosegur is not involved in the services offered by "GoSupply" and that the supplier of this platform is responsible for the access services and other circumstances related to the registration on this platform. Prosegur is only the recipient of the information that the Supplier/Contractor includes in the platform.

6.2.4. To complete its internal process of pre-classification, evaluation and pre-approval, Prosegur has implemented the service of pre-classification, evaluation and pre-approval of Suppliers/Contractors,

aimed at the continuous improvement of its Suppliers/Contractors in order to improve the sustainability and quality of the goods and services marketed to Prosegur. This service of pre-classification, evaluation and pre-approval, agreed directly between the Suppliers and Prosegur, is mandatory and involves the payment of an annual fee to Prosegur, determined according to the amount of the annual invoicing of the Supplier/Contractor and the categories of products and services to which it devotes its activity. In any case, Prosegur will determine the category assigned to the Supplier/Contractor and the corresponding annual fee, which consists of:

- Autonomous supplier: €59 per year + VAT
- Basic supplier: €99 per year + VAT
- Standard supplier: €199 per year + VAT
- Critical supplier: €299 per year + VAT

These quotas and/or the category originally assigned to the Supplier/Contractor may be changed and updated by Prosegur at any time and at its sole discretion, and the Supplier/Contractor undertakes to accept the new quotas and/or the newly assigned category as soon as they are communicated by Prosegur.

6.2.5. The Supplier/Contractor accepts that payment of the annual fees for the service of pre-classification, evaluation and pre-approval of Suppliers to Prosegur shall be made by direct debit to the same bank account indicated by the Supplier/Contractor to Prosegur for payment of invoices for works, services or supplies of goods and/or materials performed or supplied to Prosegur. Further, in the event of repayment or impossibility of payment in accordance with the foregoing, Prosegur shall be entitled to deduct and/or set off the amount corresponding to the said instalments from the invoices that have not yet been paid to the Supplier/Contractor.

6.3. Supplier/Contractor's Obligations and Liabilities

6.3.1. The Supplier/Contractor undertakes to perform the works, services and supply of goods, in accordance with what is set forth in the Order/Contract and/or its annexes and to comply with all technical, administrative, tax, labor, legal and any other obligations in connection with the contractual relationship.

6.3.2. The Supplier/Contractor shall be obliged to provide all documentation requested by Prosegur in the Order/Contract, both in terms of time and quantity, as well as any other information or documents of any kind required by the laws, rules or regulations applicable to the specified supply, work or service.

6.3.3. Upon Prosegur's request, the Supplier/Contractor shall provide evidence of compliance with the obligations set forth in the preceding paragraphs. Failure to provide such evidence or failure to provide such evidence shall constitute a serious breach of its obligations.

6.3.4. Depending on the type of order/contract, the Supplier/Contractor shall designate the persons in its organization responsible for the delivery of goods and/or performance of work and/or services in accordance with the Special Terms and Conditions and shall notify the respective Prosegur Coordinator of such designation.

6.3.5. The Supplier/Contractor and, where applicable, their subcontractors, shall be responsible for the timely payment of salaries, social security contributions and any other remuneration or compensation, labor or otherwise, that its employees are required to receive for any reason, and shall indemnify Prosegur against any claims arising from the breach of such obligation.

6.3.6. The Supplier/Contractor and, where applicable, their subcontractors, shall comply with applicable legal and other regulations, such as the fundamental conventions of the International Labor Organization relating to labor rights and social security.

The Supplier/Contractor and, where applicable, their subcontractors, shall comply with all environmental, labor, health and safety regulations in force and applicable to the Order / Contract; it shall observe Prosegur's policies and procedures and, in any case, respect Prosegur's Code of Ethics and Conduct, which is published in English at the following link on Prosegur's website:

- Prosegur Code of Ethics and Conduct - EN

6.3.7. The Supplier/Contractor and, where applicable, their subcontractors, shall be liable for and indemnify Prosegur and the rest of the Prosegur Group against claims for direct, indirect and/or consequential damages, including loss of business, loss of reputation or profits, loss or destruction of property of Supplier and/or third parties, or death, illness or injury to Supplier's and/or third parties' personnel, arising out of Supplier/Contractor's and/or its subcontractors' performance of its contractual or statutory obligations, if any. Such liability shall include attorneys' fees and court costs, without the amount of any Insurance under Clause 2.10 being a limitation of liability.

6.3.8. The Supplier/Contractor and its subcontractors, if any, shall be liable to Prosegur and the other companies of the Prosegur Group for all direct, indirect and/or consequential damages, including loss of business, image and profits, caused by him/her and the persons for whom it is legally or contractually liable, to Prosegur or the companies of the Prosegur Group by damage, Loss or destruction of their property or by death, illness or injury to their personnel, and which may be caused by any act or omission in the performance of the obligations under the Order/Contract by the Supplier/Contractor and, if applicable, its subcontractors or their personnel. Such liability shall include attorneys' fees and court costs, without the amounts of any insurance policies taken out under Clause 2.10. constituting a limitation of liability.

6.3.9. The Supplier/Contractor warrants to Prosegur indemnification against all claims of Contractor's employees involved in the performance of the Order/Contract or its subcontractors that are defended or settled by Supplier/Contractor, who shall also pay defense costs and any amounts or statements subject to settlement or included in a final judgment.

6.3.10. The Supplier/Contractor guarantees to indemnify Prosegur against any administrative or other sanctions that may be imposed on it, directly or indirectly, as a result of the execution of the Order/Contract.

6.3.11. In case of non-compliance by the Supplier/Contractor with the obligations referred to in the preceding paragraphs, Prosegur shall be entitled to deduct from the following certificates/invoices payable to Prosegur the amounts of the claims or penalties not fulfilled by the Supplier/Contractor, as well as the defense costs incurred by Prosegur as a result of the non-compliance.

6.3.12. The legal liability regime mentioned in this document does not apply to the obligations that each of the parties must comply with under the Prevention of Occupational Hazards Act or the regulations applicable to this matter and their implementing regulations, in which case the legal and regulatory regime established for such liability shall apply.

6.3.13. The liability referred to in clause 6.3.8 shall also apply during the Warranty Period and shall be equally enforceable.

6.3.14. In cases where the status of the Supplier/Contractor is held by a joint venture or an unincorporated entity other than those of its constituent parts, the liability that may arise from this Order/Contract towards Prosegur shall be of a joint and several nature for all persons or entities that are part of the entities concerned.

6.3.15. As a result of the foregoing and pursuant to the provisions of Articles 1.137 and 1.144 of the Spanish Civil Code, Prosegur may proceed individually against any of the natural or legal persons constituting the Temporary Joint Venture, or against the unincorporated entity, to demand the performance of all of the obligations set forth in the Order / Contract.

6.3.16. In no event and under no circumstances shall Prosegur be liable for any direct, indirect and/or consequential damages suffered by Supplier/Contractor arising directly or indirectly from the performance of the Order/Contract, including but not limited to loss of use, lost profits and business interruption.

6.3.17. Prosegur promotes the engagement of suppliers that meet sustainability and social responsibility criteria from companies that promote and support the United Nations Sustainable Development Goals and have some form of ESG certification, either through membership in sustainable indices or certifications in this area. Prosegur promotes and encourages suppliers and partners with whom it works to accept the following principles:

- Respect the applicable laws of all jurisdictions in which the Prosegur Group operates.
- Act as a socially responsible employer with a commitment to:
    - pay its employees a living wage that is always above the minimum wage
    - respect the prevention of child labor and forced labor,
    - respect non-discrimination and equal opportunities,
    - respect freedom of association, the right to collective bargaining and the elimination of excessive working hours.
- Ensure a safe working environment in compliance with all occupational health and safety standards.
- Use sustainable practices that respect the environment and require suppliers to make commitments in:
    - Use of renewable energy
    - Measures to reduce emissions and pollutants to avoid climate change
    - Respect for biodiversity
    - Sustainable use of natural resources
    - Waste prevention
- Respect the Prosegur Code of Ethics and Conduct

6.4. Obligations and liabilities of Prosegur

6.4.1. Payment for the goods, works and/or services at the prices and conditions stipulated in the order/contract as stipulated in clauses 2.6 and 2.7.

6.5. Assignment of the Order/Contract and Subcontracting

6.5.1. The work, goods and services that are the Order/Contract shall not be delegated or subcontracted, in whole or in part, without the prior written consent of Prosegur, which the subcontractor expressly agrees to be bound by all of the terms and conditions of this document.

6.5.2. In order to obtain subcontracting approval, the Supplier/Contractor shall require the Subcontractor to produce all documents required by the RFP and these General Terms and Conditions, as well as its written commitment to comply with each and every clause of the Order/Contract and related documents, and must immediately hand over all of it to Prosegur.

6.5.3. In the event that subcontractors are used, the Supplier/Contractor shall remain primarily liable to Prosegur for the performance of the obligations under the Order/Contract, even if it concerns goods, works and/or services directly supplied/provided by the authorized subcontractor. Notwithstanding the foregoing, Prosegur may at any time control and monitor the work of the Subcontractor and the performance of its obligations.

6.6. Economic conditions and taxes

6.6.1. The prices included in the Order/Contract and its annexes shall be considered fixed and non-revisable until the total and correct completion of the object of the Order/Contract, unless expressly stated otherwise, and shall include all taxes, charges, levies, fees and duties, present or future, with the exception of Value Added Tax or similar taxes, which shall appear separately as an independent item.

6.6.2. As an additional exception to the previous paragraph and in the event that a withholding tax is levied in accordance with the applicable legislation, the amount of the withholding tax that complies with the applicable legislation shall not be deemed to be included in the price. Thus, the Supplier pays the total amount of the invoice to the Customer and additionally pays the corresponding withholding amount to the Supplier's tax administration. In the event of a reduction of withholding tax due to the application of a double taxation treaty between the two countries, the Customer shall provide the Supplier, at the latter's request, with a certificate of tax residence within the meaning of the Agreement, so that the Supplier can pay the withholding tax applicable under the said Agreement. The Supplier, once the withholding tax has been paid, shall provide the Customer with a certificate of payment of the withholding tax paid.

6.6.3. Goods, works and/or services not included in the Order/Contract shall not be paid for if their execution has not been previously offered by the Supplier/Contractor in writing and the corresponding modification of the Order/Contract accepted, also in writing, by Prosegur.

6.6.4. Any prepayments, if any, shall be made upon presentation of an appropriate bank guarantee for the same amount payable, irrevocably and unconditionally, jointly and severally, upon first demand and waiving the benefits of excusion, order and division, and provided that such prepayments are provided for in the applicable Order/Contract.

6.6.5. Payment of the Order/Contract price shall not imply any waiver of Prosegur's rights under it.

6.6.6. The Supplier/Contractor shall be liable for any difference in freight, carriage, taxes or any other charges arising from failure to comply with the shipping instructions or any other of the conditions set forth in or applicable to the Order/Contract.

6.6.7. All taxes levied on the commercial transactions to which these General Terms and Conditions refer shall be borne by the parties in accordance with the legally established provisions. The taxpayer is responsible, in each case, for the correct taxation of its obligations.

6.7. Form of payment

6.7.1. All payments shall be made 60 calendar days after the date of the invoice, unless the parties have agreed on a different period or a different payment period is required by law. Invoices shall be paid only when Prosegur has documents evidencing satisfactory receipt of services rendered in accordance with the provisions of the Order/Contract. In case of delivery of goods, the Incoterms and/or the terms of delivery included in the Order shall apply.

The usual means of payment is bank transfer or reverse factoring.

6.7.2. The other terms of payment are precisely defined in the Special Terms and Conditions and in the Order/Contract.

6.8. Acceptance of the Order/Contract

6.8.1. Acceptance of the Contract: The signing of the contract by the parties shall be considered as full acceptance of the same.

6.8.2. Acceptance of the Order: The signature or acknowledgement of receipt as a sign of acceptance of the order by the Supplier/Contractor to Prosegur. In any case, the mere execution of the Order by the Supplier shall imply tacit acceptance of the Order by the Supplier and shall exclude any exception not accepted in writing by Prosegur.

6.9. Delivery and implementation deadlines

6.9.1. The delivery/execution term established in the Order/Contract shall be firm and shall be carried out in accordance with the quantities, dates and places specified in the delivery/execution schedules defined and supplied by Prosegur.

6.9.2. In the event that the delivery/performance deadline is exceeded, Prosegur may apply the penalties set forth and/or, if applicable, terminate the Order/Contract in accordance with clause 2.16.

6.9.3. Prosegur may change delivery/performance schedules, or order the temporary suspension of scheduled deliveries. For this purpose, it shall seek the corresponding agreement and may request the necessary adjustment of the Order/Contract.

6.10. Warranties

6.10.1. The Warranties that Prosegur may provide depending on the characteristics of the goods, works and services are as follows:

Warranty of faithful performance and fitness of the goods, work and/or services for the purpose requested. Supplier/Contractor warrants compliance with all of its contractual obligations under the Order/Contract from the time of acceptance/signature of the Order/Contract until final receipt by Prosegur of the required goods, work and/or services. Whether or not such guarantee is required shall be specified in the Request for Proposal and/or in the relevant Order/Contract.

Said Warranty shall be established through the Warranty Form in Annex II (issued by a bank with a minimum BBB- rating from Standard & Poor's or approved by Prosegur's Treasury Department) or surety insurance (issued by an insurance company with a minimum BBB- rating from Standard & Poor's or approved by Prosegur's Insurance Department) or by a direct withholding on the invoice.

6.10.2. The Supplier warrants that in case of delivery of goods that they are fully owned by the Supplier, are fit for purpose and of first quality and first use, and that they comply with the safety and quality requirements set out in the Order. The Contractor warrants that the performance of works and/or services complies with the safety and quality requirements specified in the Contract. The Supplier/Contractr guarantees compliance with the relevant applicable legislation as well as Prosegur's own standards and compliance with the work/performance programs specified.

6.10.3. The Supplier/Contractor also guarantees that the goods, works and services are free from encumbrances in favor of third parties, free from defects and suitable for their marketing/use, as well as that it has the patents, licenses and other industrial/ intellectual property rights necessary for the realization of what is the subject of the Order/Contract.

6.10.4. Warranty withholdings: Withholdings as a guarantee shall be set forth in the Order/Contract.

6.10.5. The Warranty Period for the goods, works and/or services supplied/performed by the Supplier/Contractor shall be set forth in the Order/Contract. Failing that, it will be:

For goods, 12 months from the date of commissioning or 24 months from the date of receipt of the goods at destination or from the date of delivery, according to the applicable Incoterm,whichever occurs first, if the Supplier has conditions with a longer term, they will be applied.

In the case of contracts for the performance of works and/or services, it shall be 12 months from the date of signing of the provisional acceptance certificate.

Other periods may be required if provided for in the applicable legislation and/or resulting from the particular nature of the supply, work and/or service in question.

6.10.6. During the warranty period, the Supplier/Contractor shall be liable, without prejudice to what is specified in Clause 6.3.16 and following clauses, for all breaches and/or damages resulting from the Supplier/Contractor's failure to comply with, or defective or insufficient compliance with, the terms and conditions of the contract applicable to the supply, work or service and, where applicable, for defects in the quality of the materials used.

The warranty period shall be interrupted for the time spent on the respective repairs or replacements, which in turn, once completed, shall be guaranteed for the same period as the warranty originally established.

6.10.7. Such non-compliance or defective or inadequate performance of the supply, work and/or service in question, or a quality defect, if the Supplier/Contractor has not carried out the appropriate remedial action or if it has not exercised reasonable diligence in resolving the problems raised, may result in: to the withholding by Prosegur of outstanding payments; to the execution of the financial and/or bank guarantee(s); and even up to the total or partial rejection of the executed supply, work or service, in which case the refund of the amounts paid will be requested, without this circumstance giving rise to any claim on the part of the Supplier/Contractor.

6.10.8. Prosegur shall, if applicable, deduct any contractual penalties from the invoices that have not yet been paid to the Supplier/Contractor.

Likewise, in order to compensate Prosegur for its own expenses or for the expenses and costs resulting from the engagement of third parties to remedy or execute the Supplier/Contractor's non-performance or defective performance, as well as for any other debt owed by the Supplier to Prosegur, Prosegur may deduct such amounts from the invoices that have not yet been paid to the Supplier/Contractor.

The payment or deduction of such penalties and costs shall not relieve Supplier/Contractor of its other obligations and liabilities arising under the Order/Contract.

6.10.9. Any amount claimed by Prosegur for the Supplier/Contractor's overdrafts or defaults in relation to salaries, social security, tax obligations and any other that may be required by Prosegur in accordance with legal or regulatory standards shall automatically be considered a debt owed by the Supplier/Contractor to Prosegur.

6.10.10. The possible deductions made pursuant to the preceding paragraphs are completely independent of the amount deposited as guarantee, if any.

6.10.11. If the Supplier intends to discontinue the manufacture of the Product that is the subject of the Purchase Order, it shall notify Prosegur's Purchasing Department thereof in writing with acknowledgment of receipt six months prior to the date on which it intends to discontinue the manufacture of the Product. Such notice shall contain at least the following: (i) the name of the product; (ii) the name of the orders affected thereby; (iii) a list of the countries affected; and (iv) the date on which it intends to cease manufacturing the product.

From the issuance of the Purchase Order, the Supplier guarantees adequate technical service and availability of spare parts for a period of at least ten (10) years in all countries concerned and from the date on which the product is no longer manufactured. The price of spare parts or products and services shall be offered to Prosegur at a price not exceeding the contract price of the replaced products and in accordance with the technical requirements requested by Prosegur for the product to be repaired or replaced.

In order to guarantee this obligation, Prosegur reserves the right to request from the Supplier, upon first request, a bank guarantee in accordance with the model guarantee in Annex II of this document.

In the event that the Supplier fails or is unable to comply with this guarantee, it shall have the following consequences:

- The withholding of any outstanding payment by Prosegur.
- The enforcement of the bank guarantee
- The cancelation, in whole or in part, of the Purchase Orders in progress, without any compensation in favor of the Supplier.
- The right of Prosegur to claim all damages, losses, costs and expenses (including legal fees) incurred by it in order to fulfill, by its own means or through third parties, the unfulfilled obligations of the Supplier.

In addition, the Supplier shall provide Prosegur, at its own expense, with all custom software development, including source code, object code, manuals and all other relevant information.

6.11. Insurance

6.11.1. Without prejudice to its liability under the Order/Contract and without this clause limiting the same, the Supplier/Contractor shall, at its own expense, take out and maintain at all times during the term of the Order/Contract the insurance policies described below with companies of recognized solvency. The coverages and amounts covered by such insurance shall never be less than those required by applicable law. Their maintenance shall not change the obligations to hold Prosegur harmless established in the Order/Contract.

6.11.1.1 Contracts for Work and/or Services

a) Sickness and workers' compensation insurance for all employees assigned to the Work in accordance with applicable laws, including the laws of the home country of employees working abroad.

b) Construction/building, installation and damage insurance for construction equipment rented, leased or owned by the Contractor with coverage not less than its replacement value. In the case of construction insurance, it is necessary to take out additional coverage for adjacent and existing buildings. In the event of damage and regardless of the cause, the Contractor expressly waives the right to recourse against Prosegur for damage or loss to such items and agrees to notify its insurers in writing of such waiver of recourse.

(c) Public Liability Insurance, including, but not limited to, Employer's Liability, Professional Liability, Product, Product Removal, Aftercare, and Pollution and Contamination with coverage equal to the scope of work/services agreed to in the Special Terms and Conditions of each Contract and at least equal to the lump sum amounts set forth in Annex I.

In the case of third-party liability policies issued under the time-limited coverage, the Contractor shall maintain such policies in force until the expiration of the warranty or statutory liability period. If the policies are purchased under the time-limited coverage per occurrence, the Contractor must keep the policies in force for at least two (2) years after the expiration of the warranty or statutory liability period.

Such insurance shall include Prosegur as an additional insured without losing its third party status.

d) If the use of motor vehicles, self-propelled machinery, industrial machinery, aircraft or ships is necessary for the performance of the work, third-party liability insurance with a sum insured specified in the Special Terms and Conditions of the Agreement at least equal to the standard amounts set forth in Annex I.??

If the hiring of vessels is required, protection and liability insurance from an International Group club is required (owner/charterer).

Notwithstanding the foregoing, the Contractor may obtain additional insurance as it deems necessary to fully cover its contractual obligations.

6.11.1.2 Order of Goods

a) Sickness and workers' compensation insurance for all employees assigned to the works in accordance with applicable laws, including the laws of the home country of employees working abroad.

b) Transportation insurance for the goods and/or equipment covered by the Purchase Order in accordance with the Terms and Conditions of Purchase and the Incoterm agreed to in the Special Terms and Conditions.

c) Public liability insurance, including, among others, employer's liability, professional liability, product liability, product recall, rework, and pollution and contamination, with coverage equal to the value of the goods purchased, at least the amount specified in the Special Terms and Conditions for each order.

In the case of third-party liability policies issued under the time-limited coverage, the Supplier shall maintain such policies in force until the expiration of the warranty or statutory liability period. If the policies are purchased under the time-limited coverage per occurrence, the Supplier must keep the policies in force for at least two (2) years after the expiration of the warranty or statutory liability period.

Such insurance shall include Prosegur as an additional insured without losing its third party status.

Notwithstanding the foregoing, the Supplier may obtain additional insurance as it deems necessary to fully cover its liabilities according to the Order.

6.11.2. Prior to delivery of the goods or commencement of the work/services, the Supplier/Contractor shall provide Prosegur with a certificate of insurance taken out. This certificate shall be included as an annex to the Contract/Order. Failure to provide the certificate shall give Prosegur the right to terminate the Contract/Order for a reason attributable to the Supplier/Contractor.

6.11.3. Prosegur may at any time require the Supplier/Contractor to hand over the original policies or certified copies of the insurance policies taken out by the Supplier, as well as receipts or proof of timely payment of the corresponding premiums. The Supplier/Contractor shall be obliged to deliver all this within a period not exceeding seven (7) days.

6.11.4. The Supplier/Contractor is obliged to inform Prosegur in writing of any event affecting the validity and conditions of the insurance taken out.

6.11.5. In any case, Prosegur shall never be liable for any limits, deductibles or restrictions in the terms of Supplier/Contractor's policies.

6.11.6. All insurance policies referred to in clause 2.10.1 shall include a statement releasing the insurance company from liability and non-recourse to Prosegur.

6.11.7. The Supplier/Contractor, under its sole responsibility, require Subcontractors to maintain the same liability and insurance policies as the Supplier/Contractor, if applicable. This shall not release the Supplier/Contractor from its liability towards Prosegur.

6.11.8. Depending on the scope or nature of the Contract/Order, Prosegur reserves the right to:

- Charge higher per claim limits than those set forth in Annex I.
- To require additional coverages or insurances not included in section 2.10.1.

6.12. Penalties for non-compliance

6.12.1. The penalties or sanctions for non-compliance by the Supplier/Contractor shall be specified in the Special Terms and Conditions and in the Order/Contract, otherwise they shall be subject to the applicable commercial law.

6.12.2. If not specified in the Special Terms and Conditions of the Order/Contract, the following sanctions shall be applied in case of an objective breach of the Supplier's/Contractor's obligations:

- Delivery of materials: Penalty up to 10% per week

- Delay in execution of works or provision of services: Penalty up to 5% per week.

6.13. Assignment of rights and receivables

6.13.1. The Orders/Contracts and the receivables and/or billings arising from these legal relationships may not be assigned, in whole or in part, or pledged, without the prior and express authorization of Prosegur, in writing in the form to be established.

6.13.2. Prosegur may assign, without prior consent of the Supplier/Contractor, part or all of its rights and obligations under the Order/Contract in favor of any company of the Prosegur Group or as a result of any corporate operation that involves a succession, in whole or in part, of the corresponding rights and obligations.

6.14. Inspections/Activations

6.14.1. The Supplier/Contractor shall, at its own expense, make necessary inspections prior to delivery of the goods, work or services to ensure that all requirements set forth in the Order / Contract are met.

In order to expedite arrangements to meet the delivery date, the Supplier shall have a control system in place to monitor its suppliers of materials, components, and services pertaining to the goods covered by the Order.

The Supplier/Contractor shall control, through the competent control body, the goods subject to legal requirements (technical regulations, safety, environment, etc.) and/or specified in the terms and conditions of the Order/Contract.

6.14.2. Prosegur reserves the right to inspect the goods which are the subject of the Order/ Contract and to require as many tests as necessary, at the Supplier's expense, both at the Supplier's premises and at those of its suppliers.

For this purpose, PROSEGUR shall appoint inspectors who shall have free access to the workshops and manufacturing processes, without this inspection diminishing the Supplier's responsibility.

6.14.3. The Supplier/Contractor shall conduct semi-annual inspections of these temporary facilities or workshops at Prosegur's or its customers' facilities. The Supplier/Contractor shall inform Prosegur of the results of these inspections and reviews.

6.14.4. When the Order / Contract requires the delivery of documents (drawings, specifications, etc.) to Prosegur, they must be signed in advance by the Supplier/Contractor as approval. Prosegur reserves the right to verify the accuracy of the documents and information provided by the Supplier/Contractor where they are located or where Prosegur indicates or requests it. For this purpose, Prosegur may appoint auditors who shall have free access to the documents, without such audit diminishing the responsibility of the Supplier/Contractor.

6.15. Delivery and shipment of goods

6.15.1. All goods supplied must be properly packed to avoid any damage. Prosegur will not accept any charges for packaging unless previously agreed. Goods corresponding to different Orders / Contracts shall not be packed together.

6.15.2. All shipments must be accompanied by a delivery bill or proof of delivery indicating the quantity, product description, order/contract number, supplier/contractor reference and list of packages, with distribution of the document as specified in the order/contract and/or the Special Terms and Conditions.

6.15.3. All packages shall be marked on the outside with the destination of the goods and the appropriate Order/Contract number, as well as instructions on handling or precautions to be taken in required cases.

6.15.4. In the case of goods which, due to their nature, are delivered in individual packages (e.g. laboratory products), the Supplier shall observe the following instructions:

a) Each package must be marked with the batch number, manufacture and date.
b) Goods belonging to more than two lots shall not be included in one and the same delivery, unless the Supplier has informed Prosegur in advance and it has been accepted by Prosegur in writing.
c) The Supplier shall communicate the expiry dates of the goods, if any, by indicating the expiry date of the Goods on the packaging.
d) The rules for identification, labeling, transport and handling specified in the safety data sheet, as well as the specific rules for dangerous goods.

6.15.5. In the case of goods that by their nature are delivered in tanks, the Supplier must observe and enforce the following:

(a) The duties and responsibilities of the shipper and the loading agent, both in procurement and loading operations, are governed by the provisions of applicable legislation (Land Transport Management Act, ADR Agreement, etc.).
b) The carrier accepts the performance of material loading at Prosegur's facilities.
c) The carrier is obliged to strictly comply with the regulations of the loading center (in terms of operation and safety).
d) The Supplier shall always be liable to Prosegur and third parties for any damage that may occur during loading operations within the loading center (negligent or insufficient action).
e) Before allowing access of the transport to the facilities, the Supplier must prove to Prosegur at the place of delivery that the raw material transports have the following documents:

- Insurance(s)
- Vehicle Inspection certificate (“ITV”)
- Driver's driving license and ADR
- ADR certificate for tractors and tankers
- Driver PPE
- Orange panels and danger labels.
- ADR waybill
- PPE to be used by the driver according to current regulations.

6.15.6. Prosegur's mere receipt of a delivery or shipment of goods by Supplier shall not be deemed final acceptance thereof subject to subsequent verification. Prosegur shall have the right to claim defects and/or deficiencies in quality or quantity, etc., and Supplier shall take the necessary measures to satisfy such claims.

6.15.7. The delivery of the Supply shall be subject to the Incoterm (latest edition) defined in the Special Terms and Conditions as well as in the relevant Order.

6.15.8. Prosegur reserves the right to return the goods at the Supplier's expense if they do not meet the requested specifications and quantities.

6.16. Acceptance of the work, goods and/or services

6.16.1. Preliminary Acceptance: Upon completion of the work and/or services, upon delivery of all required documents, if properly performed, and upon successful completion of all tests and installation tests, Prosegur shall issue a preliminary acceptance report indicating conformity or non-conformity with the terms and conditions set forth in the Order/Contract with respect to the work actually performed, dates of deployment, quality, proper operation, and any other observations. Upon signing of this provisional certificate, the stipulated warranty period shall commence. This provisional certificate shall be signed by the Contractor for acceptance.

6.16.2. If there are defects in the work and/or services performed, Prosegur shall set a deadline for the Contractor to remedy such defects. If this is not done within the set time limit, Prosegur may remedy the defects itself or have them remedied by third parties at the expense of the retained warranty amount, or charge the Contractor for the amount of the work and/or services not covered by the retained warranty.

6.16.3. Final Acceptance: Upon expiration of the warranty period established for the work and/or services and provided that there are no pending claims of Prosegur to be resolved by Contractor, final acceptance of the work and/or services shall take place. Prosegur shall be obliged to reimburse the Contractor for the amount, if any, of the warranty and repair funds not used for the payments to be made by the Contractor.

6.16.4. The Contractor shall, at its own expense, restore the Work that is defective due to Contractor's errors or omissions. Similarly, the cost of repair, alteration, or replacement of materials necessary to correct such errors or omissions shall be borne by the Contractor.

6.16.5. The delivery of goods, works and services and the provision of the corresponding delivery document or delivery bill does not mean that Prosegur has accepted the quality of the delivered works, goods and/or services. Notwithstanding the warranty periods indicated for each product, work or service, Prosegur shall have a period of fifteen (15) calendar days to verify the quality of the delivered works, goods and/or services and to return them at the Supplier's/Contractor's expense in case they do not comply with the quality or technical specifications required in the Order/Contract.

6.16.6. In the event that the delivery of goods, works and/or services has not been fully performed, Prosegur shall only be obliged to pay the Supplier/Contractor the price for the duly delivered works, goods and/or services accepted by Prosegur. This shall be without prejudice to Prosegur's right to require the Supplier/Contractor to fulfill its obligation to deliver the remaining work, goods and/or services or to cancel the order/contract and in any case to be compensated for the damage incurred.

6.17. Order/Contract Termination

6.17.1. The Order/ Contract is terminated by cancelation or expiration of the Order/ Contract.

6.17.2. Termination of the Order/ Contract for cause by the Supplier/Contractor.

6.17.2.1 In addition to the reasons specified by law, Prosegur reserves the right to terminate the Order/Contract for the reasons listed below as examples and without limitation:

a) The sale or transfer of the Supplier/Contractor's business inter vivos or upon death or its transformation into another legal entity in the manner provided by law without the written consent of Prosegur.

b) The Supplier's/Contractor's breach of any of the clauses or obligations contained in these General Terms and Conditions, the Order/Contract or any of the contractual documents signed by the parties.

c) The maximum penalties stipulated in the Order/Contract have been reached.

d) Failure of the Supplier/Contractor to comply with the applicable legislation.

e) The existence of embargoes and credit freezes ordered by judicial or administrative bodies of an executive nature (state authority, tax office, social security, etc.), or the dissolution of the supplier/contractor's company.

f) If more than 20% of the works, goods and services have not yet been executed /delivered, if the deadline specified in the Order/Contract has expired.

g) In case of damage or accident causing damage to persons, property or the environment.

h) Existence of serious inaccuracies in the information provided by the Supplier/Contractor, especially in relation to quality, prevention of occupational risks, health and safety, environmental management systems, conditions and compliance with work requirements.

i) Non-compliance with Prosegur's ethical and conduct rules.

j) Failure to comply with confidentiality obligations.

k) If a conflict of interest is identified between the Supplier/Contractor and an employee of Prosegur and such situation has not been previously disclosed and expressly approved.

l) If the Supplier/Contractor, its shareholders or directors are involved in cases of fraud, corruption or the commission of other offenses.

6.17.2.2 If any of the above-mentioned reasons occur, the Order/Contract shall be terminated without effect as of the date on which Prosegur notifies the Supplier/Contractor or its legal successors, if any, of its decision in this regard.

6.17.2.3 In cases where the Order/Contract may be terminated, Prosegur may take any or all of the following actions:

(a) Suspend outstanding payments.

b) Enforce the guarantees that the Supplier/Contractor may have provided.

c) Retain as a pledge the goods and elements of the Supplier/Contractor that are in PROSEGUR's possession.

6.17.3. Termination of the Order/ Contract at the will of Prosegur

6.17.3.1 Prosegur reserves the right to unilaterally terminate the Order / Contract at any time, giving reasons for its decision in writing and notifying the Supplier / Contractor at least 30 (thirty) days prior to the date on which the termination is to take effect.

6.17.4. The Supplier's / Contractor's request for a declaration of insolvency, bankruptcy, suspension of payments or opening of insolvency proceedings pursuant to the laws or regulations in force from time to time shall entitle Prosegur, within 30 (thirty) days of becoming aware of the existence of such request, to require the Supplier / Contractor to prove, within 10 (ten) days of receipt of Prosegur's request to that effect:

- That it has the necessary and sufficient material and human resources to continue the contracted work (personnel, technical means, etc.).

- That it has the necessary economic means to carry out the contracted works until their completion, for which it shall provide Prosegur, upon first request, with a directly enforceable bank guarantee, expressly waiving any rights of exclusion and division, for the total amount of the contracted works not yet carried out, increased by 25% of this amount, in order to guarantee the Supplier/Contractor's compliance with all its contractual obligations.

If the Supplier/Contractor fails to provide evidence of all the items referred to in this paragraph within the aforementioned period of 10 (ten) days, Prosegur shall be entitled to terminate the Order/Contract, with the right to be indemnified by the Supplier/Contractor for all damages that such termination of the Contract may cause.

6.18. Force Majeure

6.18.1. Neither party shall be liable for the non-performance of its obligations under the Order/ Contract to the extent that the performance thereof is delayed or rendered impossible by force majeure.

Force majeure in this sense shall mean acts of nature, unavoidable accidents, pandemics, fires, riots, acts of war, impositions, regulations, orders or actions of governments or governmental bodies and other competent authorities or other causes of a similar unforeseeable nature which are foreseeable, unavoidable, irresistible or independent of the will of the parties and beyond their control.

Notwithstanding the provisions of the preceding paragraph, the suspension of the contractual obligations caused by the personnel of the Supplier/Contractor or its subcontractors cannot be claimed as a cause of force majeure.

6.18.2. The suspension of contractual obligations shall continue as long as the cause of the force majeure continues. The party affected by the force majeure shall immediately inform the other party and shall make reasonable efforts to remedy the cause of the suspension as soon as possible.

If the cause of the force majeure lasts longer than one month, Prosegur reserves the right to cancel the Order/Contract and to pay the Supplier/Contractor the amounts due for the performance of the work, provision of services or delivery of goods performed up to the date of termination by the Supplier/Contractor, without such termination entitling Prosegur to levy any additional amount or penalty or compensation in favor of the Supplier/Contractor.

6.19. Intellectual and Industrial Property

2.19.1. Supplier's Warranties with respect to the services, products, Deliverables and Ad Hoc Developments for Prosegur.

2.19.1.1. Supplier warrants, without exception, the full and peaceful exploitation and use of the services, products, Deliverables and Ad Hoc Developments provided to Prosegur worldwide as well as (i) that the services, products Deliverables and Ad Hoc Developments for Prosegur do not and will not violate any applicable regulations or intellectual and industrial property rights or similar rights of third parties and are not subject to claims, demands or litigation; (ii) that it has sufficient authority to deliver the services, products, Deliverables and Ad Hoc Developments, and that it does not maintain any agreements or contracts with third parties that prevent it, in whole or in part, from. executing the contract to which it is bound; (iii) to obtain and assume the cost of licenses, assignments, and Intellectual and Industrial Property Rights with the mandatory scope to ensure full and peaceful exploitation by Prosegur. In compliance with the above guarantee, the Provider exempts Prosegur from all liability for infringements related to the exploitation and use of the services, products, deliverables and Ad Hoc Developments for Prosegur provided by the Provider that Prosegur may incur.

Thus, the Supplier must obtain the prior express written consent of Prosegur to incorporate into the services, products, deliverables and Ad Hoc Developments for Prosegur, of any third-party element, including those protected by Intellectual and Industrial Property Rights.

2.19.1.2. The Supplier guarantees Prosegur and is obliged to provide documentary proof to Prosegur, if required, that it has the Intellectual and Industrial Property Rights necessary for the execution of what is the object of this Contract.

2.19.1.3. The Supplier undertakes to notify Prosegur of any information it has regarding claims from third parties in relation to the Intellectual and Industrial Property Rights on the services, products, Deliverables and/or Ad Hoc Developments for Prosegur, or that may affect Prosegur's rights, and will refrain from initiating any action without the prior written consent of Prosegur.

2.19.2 Indemnity

In the event that any claim, judicial or extrajudicial, is filed against Prosegur, related to the infringement of the Intellectual and Industrial Property Rights used by the Supplier or as a result of any action, claim or procedure, public or private, that is initiated because of actions, both by action and by omission, carried out or permitted by the Supplier or by any of its directors, agents or employees, in relation to the fulfilment of the obligations hereby referred, the Provider exempts Prosegur from all liability and will indemnify Prosegur for the damages suffered, undertaking to hold it and its directors, officers and employees harmless from any loss, liability, damages, expenses and costs (including legal costs) incurred by Prosegur, as well as from any damage caused to third parties, guaranteeing Prosegur to continue using the Intellectual and Industrial Property Rights that caused the claim or making available other different ones that allow the continuation of the services, products or the contract.

2.19.3. Intellectual and Industrial Property Rights of Prosegur.

2.19.3.1. Intellectual and Industrial Property Rights shall be understood as any intellectual and industrial property right or of a similar nature on any results that are or may be subject to protection in accordance with the regulations for that purpose. The Supplier undertakes to respect the Intellectual and Industrial Property Rights and any other of a similar nature owned by Prosegur, and acknowledges that nothing in this document is a transfer, assignment or license over such in favor of the Supplier. The Supplier acknowledges that it may only use Prosegur's Intellectual and Industrial Property Rights with its express instruction and written consent, and only within the framework of the execution of the contract, being obliged to respect Prosegur's instructions.

2.19.3.2. In particular, the Supplier may not use the name, trade name, logo or trademarks of Prosegur, nor may use them or use the acceptance of any offer, nor the subscription or execution of this Contract, nor the provision of the services referred to therein, as a reference for the acquisition of new customers or business acquisition or to maintain a certain professional level.

2.19.4. Ownership of the Rights over potential Ad Hoc Developments of the Supplier for Prosegur.

2.19.4.1. In the hypothetical event that as a result of the relationship between the parties, the Supplier must carry out an Ad Hoc Development for Prosegur, Prosegur will be the exclusive owner, without geographical or temporal limit, of all the Intellectual and Industrial Property Rights over said Ad Hoc Developments that the Supplier, or any person whom the Supplier has contracted for that purpose, has developed for Prosegur as a result of the relationship regulated herein.

In the event that the ownership of the Intellectual and Industrial Property Rights over the Ad Hoc Developments for Prosegur could not be originally attributed to Prosegur in accordance with the current legislation, then, by virtue of this document, the Supplier assigns to Prosegur the ownership of all Intellectual and Industrial Property Rights, on an exclusive basis, and with the maximum extent permitted by law, that is, for the entire duration of the Intellectual and Industrial Property Rights assigned, wordlwide and for any type of exploitation, even if it is not the usual sector of activity of Prosegur. Consequently, Prosegur may freely exercise in the manner it deems the Intellectual and Industrial Property Rights of the Ad Hoc Developments, including its exploitation, transmission, assignment, license to third parties, and all under the terms and conditions it considers.

2.19.4.2. The Supplier undertakes to collaborate with Prosegur to give effect to its obligations, and in particular (i) to collaborate in obtaining the registrations relating to the Intellectual and Industrial Property Rights of Prosegur (ii) to immediately inform Prosegur of any results obtained within the framework of the contractual relationship with Prosegur, providing all the documentation and other support necessary to guarantee Prosegur’ s ownership of the Ad Hoc Developments for Prosegur.

2.19.4.3. The Supplier acknowledges that the remuneration agreed in favour of the Supplier also satisfies the obligations and commitments assumed by it in this clause, renouncing to claim for them.

2.19.5 Software.

2.19.5.1. In the hypothetical event that the Provider licenses Standard Software (that developed generically for the same use by a multitude of people) to Prosegur for the execution of this agreement, said license will be exclusive, irrevocable, sublicensable for use (including in favor of the Prosegur Group), worldwide and for the maximum term of such rights.

2.19.5.2. The Provider guarantees that it will not use open source software (under an open source license) for the execution of this agreement without the prior written consent of Prosegur. To this end, it will inform Prosegur of the terms and conditions of the applicable license, confirm that the computer program as a whole cannot be considered as open source software, and that its use does not restrict the use of the services, products, Deliverables and Ad Hoc Developments for Prosegur. In case of authorized use, the Provider undertakes and guarantees compliance with the terms and conditions of the applicable license.

2.20. Data confidentiality and documents

2.20.1. Confidential information is considered to be information that is protected from access by unauthorized persons, and in particular:

a) All information (written or oral) and materials of any kind shown or made available (before or after the date of the Order/Contract) by Prosegur or its directors, employees, agents, subsidiaries or by its consultants, lawyers, auditors or external suppliers or processed in the course of the activities that are the subject of the Order/Contract, as well as all information to which the Supplier/Contractor has access or of which it becomes aware during the performance of the Services that are the subject of the Order/Contract, has access to or obtains knowledge of, and, in any case, any data relating to or connected with an identified or identifiable natural person, whether it is information or material relating to Prosegur or to third parties (whether it is information or data relating to customers, suppliers, employees or other third parties connected in any way with Prosegur or any of the companies or entities of the Prosegur Group);

b) The content of the service, the existence of prior discussions and negotiations between Prosegur and the Supplier/Contractor, the existence of any offer of goods, works and/or services, of any document accepting an offer of goods, works and/or services or any other agreement, contract or document relating to or aimed at the provision of goods, works and/or services by Supplier/Contractor to Prosegur, and the content of such discussions, negotiations, offers of goods, works and/or services, letters, contracts, agreements, contracts or documents.

c) including, but not limited to, the Prosegur Group's operations, trade secrets, business secrets, ideas, business plans, expansion plans, marketing or sales information, new business opportunities, development projects, intellectual and industrial property rights, any scientific or technical information, inventions, designs, processes, procedures, formulas, improvements, technologies or methods;

concepts, samples, reports, data, know-how, work in progress, designs, drawings, photographs, development tools, specifications, computer programs, source code, object code, organizational charts and databases, whether the information is in written, documentary, oral, visual, electronic, machine-readable, sample, model or other form. The Parties hereby agree that Confidential Information need not be new, unique, patentable, copyrightable or a trade secret to be considered Confidential Information and thus protected.

Hereinafter, all information referred to in paragraphs a), b) and c) shall be referred to as “Confidential Information”.

2.20.2. Obligation of confidentiality:

a) The Confidential Information shall be kept confidential by the Supplier/Contractor and shall not be disclosed, in whole or in part, directly or indirectly (through its employees, external or internal collaborators, subcontractors, auditors or other affiliates) to any third party, unless previously agreed in writing by Prosegur. In particular, the Supplier/Contractor undertakes to take the necessary measures to prevent unauthorized third parties from accessing the Confidential Information and to restrict access to such information to authorized employees who need such information for the performance of the goods, works and/or services and to impose the same obligation of confidentiality on them.

b) The Supplier/Contractor warrants that the Confidential Information shall be used or exploited for its own benefit or for the benefit of any third party for any purpose or purposes other than the performance of the goods, works and/or services.

c) The Supplier/Contractor agrees not to copy, distribute, disclose, lend or otherwise reproduce, disclose or transfer the Confidential Information to any third party, nor publish or otherwise make it available, either directly or through any third party or company, to any third party, without Prosegur's prior written consent.

d) The Supplier/Contractor undertakes that all Confidential Information to which it has access shall remain on Prosegur's premises and shall not be transferred to any other location unless Prosegur has given its prior written consent thereto.

e) The obligations imposed on the Supplier/Contractor in the Order/Contract shall also be binding on its employees, external and internal collaborators, subcontractors, lawyers and auditors, and therefore the Supplier/Contractor shall be liable to Prosegur if such obligations are breached by such employees, collaborators, subcontractors, lawyers and auditors. The Supplier/Contractor agrees to obtain from its outside employees or subcontractors authorized by Prosegur a written undertaking with respect to the Confidential Information in their possession identical to the terms set forth in this clause.

2.20.3. Exceptions to the confidentiality obligation. Audits:

a) The confidentiality obligation shall not apply and, therefore, information that is or becomes available to the public for reasons other than a breach of the Confidentiality Obligation by the Supplier/Contractor; that has been disclosed prior to the date of the Order/Contract; that is already in Supplier's lawful possession and is not the subject of a confidentiality agreement between the Parties, provided that such fact is disclosed to the other Party prior to the date of disclosure, shall not be considered Confidential Information; obtained by a third party without restriction and without breach of any legal or contractual obligation of the third party; or independently developed by the Supplier/Contractor for purposes other than the goods, works and/or services to be provided to Prosegur and developed without the use or support of Confidential Information.

b) Disclosure of confidential information pursuant to a court or administrative order shall not be subject to the confidentiality obligation provided herein, provided that the Supplier/Contractor who received the relevant order has previously informed Prosegur in writing of the obligation to disclose.

c) Prosegur is entitled to monitor the development of the ordered goods, works and/or services to make sure that they comply with the instructions given and the regulations in force. It may request from the Supplier/Contractor any information it deems relevant, obtain access to the place where the Services are being developed and carry out, directly or through third parties, as many audits and verifications as it deems interesting.

2.20.4. Return of Confidential Information: Upon completion of the work or delivery of goods and/or the provision of the service that is the subject of the Order / Contract, or before that date if so requested by Prosegur and it is not necessary for the Supplier/Contractor to have them in order to provide the services to Prosegur, the Supplier/Contractor shall return to Prosegur any Confidential Information that is in the possession of the Supplier/Contractor.

2.20.5. Ownership of Confidential Information: No right or title of ownership or any other right over the Confidential Information is recognized in favor of the Supplier/Contractor, except for the rights of use stipulated in the Order/Contract and with the limitations indicated therein.

2.20.6. Duration: The duration of these confidentiality obligations shall be perpetual and shall remain in effect after the termination of the relationship between Prosegur and Supplier/Contractor for any reason.

2.20.7. Breach: The Supplier/Contractor shall be liable for all damages incurred by Prosegur as a result of the breach of any of the confidentiality obligations established.

2.20.8 The performance of the Services that are the subject of a service offer by the Supplier or by a subcontractor hired by the Client shall in no case impede the supervisory powers of the Bank of Spain and/or other supervisory authorities with respect to the Client's activity. The Supplier undertakes to grant the Banco de España and other supervisory authorities direct and unrestricted access to the Client's information held by the Supplier or its subcontractors hired by the Client, so that the Banco de España or other supervisory authorities may carry out the appropriate checks in relation to such information at the Supplier's or its subcontractors' premises, including verifying the suitability of the systems and applications used. The Supplier undertakes to obtain from its subcontractors hired by the Client a written commitment identical to the conditions established in this provision with respect to the information in their possession, access to their premises and verification of the suitability of the systems and applications used.

6.21. Personal data protection

6.21.1. If the Supplier needs to access personal data held by Prosegur, it will be necessary to sign the Data Processing Agreement, which can be found in Annex III.

6.21.2. In any case, the Supplier that needs to access personal data held by Prosegur (hereinafter “Data”) shall be subject to compliance with the legal regime provided for in Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27. April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/ EC -General Data Protection Regulation- (hereinafter “GDPR”), as well as the Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD).

In general, the Supplier who has access to personal data expressly declares and undertakes to do so in compliance with applicable data protection legislation:

a. To use and process the Data solely for the purpose of fulfilling this Agreement and, in any case, to comply with the instructions received from Prosegur. The Supplier expressly refrains from using the Data for any use other than the agreed use and, in particular, from modifying them, using them for its own business interests or transmitting them or making them available to third parties, including for storage purposes.

b. To treat the personal data provided by Prosegur in connection with the development of the subject matter of the contract with strict confidentiality and restraint and to undertake not to disclose such data to third parties, as well as any other information provided to Prosegur.

c. To return to Prosegur, upon termination of the provision of services under this Agreement, all documents and files in which the Data are contained, in whole or in part, regardless of their medium or format, as well as copies thereof.

d. To limit the access and use of the Data to its employees, agents and collaborators whose access and knowledge is strictly necessary for the development of the object of the contract, being obliged to impose on them the obligation of confidentiality and prohibition of use in relation to the Data, under the same conditions as those provided for in this contract, and agreeing to be liable for any breach of said obligations on the part of its employees, agents and collaborators.

e. To adopt, implement and require the necessary technical and organizational security measures to ensure adequate security of Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage through the application of appropriate technical or organizational measures ("Integrity and Confidentiality"), as well as to update the security measures in accordance with the legal requirements that arise during the term of this Agreement, and any others subject to verifiable notice by Prosegur.

   In particular, pursuant to Article 32 of the GDPR, the Supplier shall implement the technical and organizational measures appropriate to ensure a level of security appropriate to the risk, taking into account the degree of sensitivity of the Data and the Processing Activities carried out, including but not limited to the following:

   - the pseudonymization and encryption of personal data where appropriate;
   - the ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;
   - the ability to promptly restore availability and access to personal data in the event of a physical or technical incident;
   - a process for periodically reviewing, evaluating and assessing the effectiveness of technical and organizational measures to ensure the security of processing.

f. The Supplier shall not subcontract any of the services which are the subject of this Agreement and which involve the processing of Personal Data, unless expressly approved in writing in advance by Prosegur.

In the event that the subcontracting of any Processing is required, Prosegur must be notified in writing in advance, specifying the Processing to be subcontracted and clearly and unambiguously identifying the company carrying out the subcontracting and its contact details.

In case of authorization, the subcontractor, which also has the status of a Data Processor, shall also be obliged to comply with the obligations set forth in this Agreement for the Supplier and the instructions issued by Prosegur. It is the responsibility of the original supplier to regulate the new relationship in accordance with Article 28 of the GDPR, so that the new processor is subject to the same conditions (instructions, obligations, security measures...) and the same formal requirements as he is, in terms of proper processing of personal data and ensuring the rights of data subjects.

In case of non-compliance by the sub-processor, the original supplier shall remain fully liable to Prosegur with regard to the fulfillment of the obligations.

g. If the Data Subjects exercise their rights of access, rectification, erasure, objection, non-submission to automated individual decisions, restriction of processing and data portability against the Supplier, the latter must notify them by e-mail to the address provided by Prosegur. The notification must be made without undue delay, but no later than on the business day following receipt of the request, together with any other information that may be relevant to the resolution of the request, if applicable.

h. If there is a breach of security of personal data, the Supplier must report it immediately and in any case before the expiry of the maximum time limit of twenty-four (24) hours, through the contact address (physical or electronic) indicated by Prosegur during the development of the contractual relationship between the Parties, together with all relevant information for the documentation and communication of the incident.

6.21.3. To indemnify Prosegur against all claims that may be brought against Prosegur before the appropriate supervisory authority, arising from a breach by Supplier and/or its subcontractors of the provisions of this Agreement and the applicable legislation on the protection of personal data, and to undertake to pay the amount to which Prosegur may be ordered to pay under penalties, fines, compensation, damages and interest, including legal fees incurred on the occasion of the aforementioned breach.

6.22. Information technology security

The Supplier undertakes to support an operating system with the latest security updates, at least those of the last three months. It also guarantees that it has installed antivirus software that is up to date and whose automatic updating is enabled.

The Supplier shall not connect from a computer not owned by Prosegur to perform administrative tasks on Prosegur's servers.

Were there a breach of these obligations, Prosegur shall, to the extent permitted by law, be excluded from any liability for direct and indirect damages of any kind, including but not limited to loss of profit or loss of customers, profits or exploitation opportunities, resulting from a breach of security of equipment/computer systems or communication networks of the Supplier, including situations of leakage of information or falsification of information, intrusion or illegal penetration of systems,

communications and/or software by malware (viruses, Trojans, worms) and other harmful third party programming routines, without limiting this enumeration to other possibilities that may alter and/or compromise Prosegur's computer or communications systems.

Supplier shall have unlimited liability for damages of any kind, direct or indirect, including but not limited to loss of profits or loss of customers, profits or exploitation, for any interruption, disruption or failure of service provided to Prosegur caused by acts or omissions of third parties due to breach of these obligations.

Should the Supplier discover a breach of the security of its systems, it must inform Prosegur's Project Manager within 24 hours of becoming aware of it in a manner that allows a record to be kept. Compliance with this obligation shall not release the Supplier from liability for non-compliance with the above obligations.

The Supplier shall comply with the provisions of the Annex V Use of IT Resources and Systems and sign the Annex "*USER STATEMENT ON THE USE OF IT RESOURCES AND SYSTEMS",* which is part of this document.

Any supplier requiring access to the Prosegur Group's information technologies, offering technological and/or digital services/products, as well as non-technological services that have the ability to access the Group's information technologies and/or information, must comply with the provisions of Annex IV. Should the Supplier provides services that do not require access to the information technologies of the Prosegur Group, those headings of the Annex that allow for an assessment of the Supplier's risk to be assessed in relation to Prosegur shall apply.

2.22.1 Audit

Information Security reserves the right to conduct technical audits and verify the status of Supplier's compliance with the control scheme established by Supplier.

With respect to the technical audits, the costs and expenses associated with Prosegur's intervention shall be borne by Prosegur. If vulnerabilities are discovered, the Supplier shall be responsible for remediation in accordance with Prosegur Group's technical vulnerability management procedures and in accordance with the following resolution times:

- Critical: 10 days.
- High: 20 days.
- Medium: 90 days.
- Low: 180 days.

If the deadlines are not met, a penalty of 5% of the total annual billing will be applied, to be set off in future invoices associated with the service.

6.23. Settlement of Disputes and Disagreements

6.23.1. The law applicable to the Order/Contract is the law of the place of performance. The place of performance shall be the place where, in accordance with the Order/Contract, the goods are to be delivered or the work is to be performed and/or the services are to be rendered.

6.23.2. In the absence of an agreement, the goods shall be deemed to be delivered and the work and/or services shall be deemed to be performed at the place where the relevant company of the Prosegur Group that signed the relevant Order/Contract has its registered office from a legal point of view.

6.23.3. For any disagreement that may arise in relation to the interpretation, execution or performance of the Order/ Contract, the parties expressly submit to the jurisdiction of the ordinary courts of the city where the registered office of the Prosegur Group company that signs the corresponding Order/ Contract is located.

6.24. Files

6.24.1. The Supplier/Contractor is obliged to keep a complete record of the goods delivered and/or work performed and/or services rendered under the Order/Contract, as well as of all related transactions. The Supplier/Contractor shall maintain all such records for a period of at least three years after completion of the Order/Contract. These records must be available for possible audit by Prosegur. The audit, if applicable, does not apply to the Supplier/Contractor's patents or additional information related to them.

6.24.2. With the aim of increasing the requirements for its suppliers in terms of sustainability, Prosegur reserves the right to audit the environmental, labor and corporate governance policies of its main suppliers.

7. ANNEXES

7.1. Associated Documents:

Code	Name
DS-GLO-EF-COM-02	Annex I: List of insurance limits according to products or services
MD-GLO-EF-COM-02	Annex II: Model of bank guarantee of faithful performance and guarantee of goods, works and/or services
MD-GLO-LEG-07	Annex III: Data Processing Agreement
	Annex IV: Technological Risk and Cybersecurity Requirements
	Annex V: Use of Prosegur IT Resources and Systems

7.2. ANNEX I: LIST OF LIMITS DS-GLO-EF-COM-02

AMOUNTS PAYABLE UNDER INSURANCE POLICIES ACCORDING TO PRODUCTS OR SERVICES (PER CLAIM)

ACTIVITY	PYMC	MULTINATIONAL
ALL		
Accident Insurance:	Legal minimum	Legal minimum
Civil Liability Insurance for the operation of the activity or work performed	3.000.000 €	6 000 000 €
Product liability, product recall, post-work, bonding and mixing, pollution and contamination	3.000.000 €	6 000 000 €
Employer's Liability Insurance	300.000 €	600.000 €
Liability for automobiles, self-propelled machinery, aircraft, boats:	Legal minimum	Legal minimum
Insurance adapted to the place of service		
CONSTRUCTION		
Construction/Building and Assembly Insurance:	Construction budget	Construction budget
Product liability, product recall, post-work, bonding and mixing, pollution and contamination	3.000.000 €	
Industrial Machinery Liability:	3.000.000 €	6.000.000 €
Own damage to construction equipment; rented or owned by the Contractor:	Replacement value	6.000.000 €
Ten-year insurance:	Legal minimum	Replacement value - Legal minimum
PROFESSIONAL SERVICES		
Professional Liability Professional activity rendered	3.000.000 €	6.000.000 €
Cyber risks and data protection	3.000.000 €	6.000.000 €
TECHNOLOGICAL PROFESSIONAL SERVICES		
Professional Liability Tech PI	3.000.000 €	6.000.000 €
Cyber risks and data protection	3.000.000 €	6.000.000 €
TECHNOLOGY		
Professional Liability Tech PI	3.000.000 €	6.000.000 €
Product liability, product recall, post-work, bonding and mixing, pollution and contamination	3.000.000 €	6.000.000 €
Cyber risks and data protection	3.000.000 €	6.000.000 €
TRANSPORTATION OF PURCHASED GOODS		
Door-to-door transportation coverage Loading and unloading transportation	Value transported	Value transported
STOCK STORAGE IN SUPPLIER WAREHOUSES		
All-risk coverage warehouse	Value transported	Value transported
PRODUCT AND SERVICE WARRANTY		
Product warranty	Legal minimum	Legal minimum
Product recall		
Stock out guarantee		
Customer liability		
Loss of profit / loss of business		

7.3. ANNEX II MODEL GUARANTEE MD-GLO-EF-COM-02

The entity [•] (hereinafter, the □BANK□), provided with tax number [•] with domicile in [•], and in its name and on his behalf Mr. [•] and Mr. [•] with sufficient powers to bind it in this act according to the power of attorney granted by the Notary of [•], Mr. [•], on [•] of [•], [•], with notarial record no. [•]

GUARANTEES

Unconditionally, irrevocably and jointly and severally, expressly waiving the benefits of division, excusion and order, up to the limits and under the conditions indicated below, to [ ] (hereinafter [SUPPLIER]), located in [ ] and with tax identification number [ ], for payment by the SUPPLIER to PROSEGUR COMPAÑÍA DE SEGURIDAD, S.A. (hereinafter "PROSEGUR") for all the obligations assumed by the SUPPLIER in the Agreement of [ ] dated [ ] (hereinafter "AGREEMENT"), under which the SUPPLIER [ ] to PROSEGUR (hereinafter [GOODS] [WORKS] [SERVICES]) and, in particular, for the payment of losses, damages, claims, causes of action, liabilities, penalties, sanctions, fines, costs and/or quantified and determined expenses of any nature whatsoever incurred by SUPPLIER against Prosegur or attributable to Prosegur as a result of SUPPLIER's liability now or in the future, as a result of misleading or inaccurate information, breaches, contingencies and/or third party claims arising from the performance of the AGREEMENT.

ONE. - IMPLEMENTATION. This bank guarantee shall be enforced upon PROSEGUR's first request for payment, one or more times, up to a maximum amount of [•] ([•]) EUROS against PROSEGUR's claim, accompanied by a copy of the request for payment sent by PROSEGUR to the SUPPLIER and proof that ten (10) business days have elapsed since the sending of said request for payment without the SUPPLIER having paid the corresponding amount.

The BANK undertakes to transfer the amount claimed, up to the maximum amounts (individually and collectively) set forth above, to the account specified by PROSEGUR for this purpose within a non-extendable period of three (3) days after receipt of such notice.

TWO. - WAIVER OF EXCEPTIONS. This Guarantee is irrevocable and is granted in the abstract and at the first demand, the BANK may not oppose or allege against PROSEGUR any type of exception and, in particular, the personal exceptions that the SUPPLIER could prove against PROSEGUR. Thus, once the request described in the previous section has been presented, the BANK may in no way question the validity of the claim to the BANK against PROSEGUR.

THREE. - TERM OF VALIDITY. This guarantee shall become effective as of today's date and shall be valid for […] ([…]) years as of today's date. After said date, if the BANK has not received any reliable communication of payment of the amount made by the SUPPLIER, it shall expire and shall be automatically terminated.

FOUR. - ASSIGNMENT. PROSEGUR may assign this guarantee to any third party. For such assignment to be effective vis-à-vis the BANK, it is sufficient that it be communicated by PROSEGUR to the BANK. In such case, all references in this guarantee to PROSEGUR shall be deemed to refer to the assignee of this guarantee.

FIVE. - EXPENSES. All costs and expenses in connection with this bank guarantee shall be paid and borne solely by SUPPLIER.

This guarantee has been registered on the same date in the Special Guarantee Register under number [•].

[*NOTARIZED*]

7.4. ANNEX III. DATA PROCESSING AGREEMENT

BY AND BETWEEN

PROSEGUR (hereinafter, the "Data Controller") and the Supplier (hereinafter the "Data Processor"), collectively referred to as the "**Parties**" and individually as the "**Party**"

RECITALS

I. Whereas, as a consequence of the provision of the services detailed in the Purchase or Supply Agreement, the Data Processor may have access to personal data that are under the responsibility, custody and protection of **PROSEGUR**; having for these purposes the Supplier the legal status of Data Processor.

II. Whereas, consequently and in full compliance with the provisions of the applicable national and Community regulations, the Parties wish to include in this Agreement the conditions for the processing of data by the Supplier, in accordance with the provisions of Spanish law.

III. Whereas, without prejudice to the foregoing, the Parties also wish to comply with the requirements established by Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the regulation of the relationship between data processors, and to this end they sign the following

CLAUSES

One. Personal data processing

The provision of services may involve access by the Data Processor to confidential information and personal data under the responsibility of PROSEGUR. In this sense, the Supplier will be considered as the Data Processor, and its processing of personal data under the responsibility of PROSEGUR will consist solely and exclusively of accessing and, where appropriate, storing the personal data strictly necessary to provide the services referred to in the Purchase or Supply Agreement.

Two. Confidentiality and duty of secrecy

Unless otherwise agreed by the Parties, the Parties and the other companies belonging to or associated with their group shall maintain absolute confidentiality about this contract, their business and the information and documents about the other party that have come to their knowledge in the course of the performance of the contract. Likewise, the Data Processor expressly undertakes to keep confidential all information under the responsibility of the Controller or third parties to which it has access in connection with the provision of its services, and undertakes to keep such data confidential.

To this end, the Data Processor undertakes to take the necessary measures vis-à-vis its employees or collaborators to ensure that they are informed of the need to comply with the obligations incumbent on it as Data Processor and with which they must therefore comply, as well as to ensure that the personal data of which it becomes aware under this Agreement remain confidential even after this Agreement has been terminated, for whatever reason. To this end, the Data Processor shall give all necessary warnings (through training, awareness, etc.) and sign the necessary documents with its employees or collaborators to ensure compliance with these obligations. The latter must be informed

in an understandable manner of the existence of this agreement, the security rules that affect the performance of their duties, the consequences of non-compliance and the confidentiality of the information and the obligation to keep personal data confidential, with the obligation of confidentiality and secrecy continuing even after the termination of the relationship with the Data Processor.

This duty to inform the Data Processor's employees and collaborators shall be carried out in such a way as to document and make available to PROSEGUR the fulfillment of this duty.

In addition, confidential information and documents may not be used for any purpose other than the fulfillment of the purpose of the agreement, unless such information is generally known and is information required by law or other applicable and mandatory regulation.

Upon termination of this agreement, the obligation of confidentiality and non-disclosure provided for in this clause shall survive indefinitely, even after the termination of the relationship with the Data Controller for any reason.

If a person performing professional functions for the Data Processor detects any type of improper behavior (access to information that does not correspond to their function, improper use of users and passwords, a user with more privileges than necessary or other), the Data Processor shall be obliged to notify PROSEGUR immediately and provide a detailed report of the facts.

Three - Instructions from the Data Controller

The Data Processor undertakes to process the Personal Data to which it has access only in accordance with the written instructions given to it for this purpose by the Data Controller, following, at least, the same measures for the protection of the Personal Data and the security of its storage that PROSEGUR applies for this purpose. This obligation also applies to the international transfer of personal data to a third country or an international organization.

Consequently, the data known or obtained by virtue of this agreement:

- may not be used for purposes other than the execution of the same, are confidential and may not be published or disclosed to third parties without the prior written consent of the Data Controller. Under no circumstances will the data be processed for its own purposes.
- will not be disclosed to third parties without the prior written consent of PROSEGUR. In this sense, before PROSEGUR authorizes the transfer, the Data Processor must specify in writing the entity or entities to which the data will be transferred, the data or the category of personal data that will be the subject of the transfer, and the security measures that will be taken to carry out the transfer.

In this context, the Data Processor undertakes to inform the Controller without undue delay if any instruction given by the Controller may violate applicable Community or Member State data protection provisions.

In the event that the Data Processor uses the Data for any other purpose, discloses it or uses it in violation of the provisions of this agreement, it shall also be considered the Data Controller and shall be personally liable for the violations it commits and for the damages it causes PROSEGUR in such case.

Four. Subcontracting of services

The Data Processor shall not subcontract any of the services which are the subject of this Agreement and which involve the processing of Personal Data, unless expressly approved in writing in advance by Prosegur.

In the event that the subcontracting of any Processing is required, Prosegur must be notified in writing in advance, specifying the Processing to be subcontracted and clearly and unambiguously identifying the company carrying out the subcontracting and its contact details.

In case of authorization, the subcontractor, which also has the status of a Data Processor, shall also be obliged to comply with the obligations set forth in this Data Processing Agreement and the instructions issued by Prosegur. It is the responsibility of the original Data Processor to regulate the new relationship in accordance with Article 28 of the GDPR, so that the new processor is subject to the same conditions (instructions, obligations, security measures...) and the same formal requirements as he is, in terms of proper processing of personal data and ensuring the rights of data subjects.

In case of non-compliance by the sub-processor, the original Data Processor shall remain fully liable to Prosegur with regard to the fulfillment of the obligations.

Five. Security measures

The Data Processor undertakes to comply with the security measures of an organizational and technical nature, suitable to ensure a level of security appropriate to the risk that may arise from the processing, in order to ensure the security and integrity of personal data and prevent their alteration, loss, unauthorized access or processing, taking into account the state of the art, the cost of the application, the nature of the data stored, the scope of the processing and the risks to which they are exposed and the impact this could have on the rights and freedoms of natural persons, whether resulting from human action or from the physical or natural environment, thus meeting the requirements of applicable legislation.

The Data Processor shall be subject to security measures appropriate for the protection of the Personal Data and other information to be processed by it, in accordance with the outcome of the risk assessment carried out by PROSEGUR, taking into account the state of the art, the cost of implementation, the nature of the data stored, the scope and purposes of the processing and the risks to which they are exposed. The Data Processor shall provide PROSEGUR with the necessary information in cases where the risk analysis carried out by PROSEGUR or by the Data Processor shows that the Processing involves a high risk.

As a result, the Data Processor shall apply to the Personal Data subject to the Processing Operations at least the measures listed at APPENDIX I of this Agreement.

Six. Notification of security breaches

The Data Processor shall ensure the implementation of the security requirements set forth in this Agreement and notify PROSEGUR of any incident that directly or indirectly affects the information, documentation and Personal Data under PROSEGUR's responsibility.

If the Data Processor or any person involved in the services becomes aware of an incident resulting in theft, loss or damage to the Data, that a person has accessed the Data without authorization, or

that the Data has been used inappropriately, the Data Processor shall notify PROSEGUR of the details of the incident without undue delay and in any event within twenty-four (24) hours, by e-mail to dpo@prosegur.com, attaching all relevant information for the documentation and notification of the incident and, at a minimum, the following information (if available):

1. Description of the nature of the personal data security breach, including, where possible, the categories and approximate number of data subjects affected as well as the categories and approximate number of personal data records affected.
2. The name and contact details of the data protection officer or other point of contact from who further information can be obtained.
3. Description of possible consequences.
4. Description of the measures adopted or proposed to correct the personal data security breach, including, where appropriate, the measures to mitigate any possible negative effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

It will be the responsibility of the Data Processor to take the necessary measures to contain and remedy the incident.

PROSEGUR will regularly monitor the status of the remediation of the incident, and the Data Processor agrees to provide the requested reports.

Seven. Register of categories of processing operations

The Data Processor shall, where required by the General Data Protection Regulation and other relevant legislation, keep a written register of all categories of processing operations carried out on behalf of PROSEGUR reflecting:

1. The contact details of both PROSEGUR and the Data Processor, as well as those of their representatives and Data Protection Officers, if any.
2. The categories of processing operations carried out on behalf of PROSEGUR.
3. Where applicable, any international data transfers that may take place in the context of the specific processing.
4. A general description of the technical and organizational measures to be applied.

Eight. International Transfers

In general, the Data Processor shall not make international transfers of data under the Data Controller's responsibility outside the European Economic Area, unless the Data Controller has given its prior written consent.

If the Data Processor is required by applicable Union law or Member State law to transfer Personal Data to a third country or international organization, it shall inform the Data Controller in advance of such legal obligation, unless the law prohibits it for important reasons of public interest.

If the Controller authorizes the aforementioned international data transfers and the data is to be transferred to a country that does not have an adequate level of protection or an equivalent level of protection, the standard contractual clauses established by the European Commission for this purpose must be signed. The Data Processor shall facilitate these procedures to the Data Controller prior to the international data transfer.

Nine. Rights of data subjects

The Data Processor shall assist the Controller by implementing appropriate technical and organizational measures and according to the nature of the data processed in relation to requests aimed at exercising the rights of data subjects, in particular their rights of access, rectification, erasure ("right to be forgotten"), objection to the processing of their data, request for portability of their personal data, restriction of processing and the right not to be subject to automated individual decision-making, including profiling.

If the data subjects exercise the rights referred to in the preceding paragraph vis-à-vis the Data Processor, the latter must notify them by e-mail to the address protecciondedatos@prosegur.com. The notification must be made without undue delay and no later than on the business day following receipt of the request, accompanied, where appropriate, by any other information that may be relevant to the clarification of the request.

Ten. Return or Destruction of Data

After the performance of the contractual service, the Data Processor undertakes to return to Prosegur the Personal Data and, if applicable, the data carriers on which they are stored, as soon as the service has been performed. The return must entail the total erasure of the existing data in the computer equipment used by the Data Processor.

The Data Processor must also ensure that upon termination of the contractual relationship with a person with whom it performs a professional function:

- the person returns the information and data carriers from PROSEGUR and does not retain them in any form.
- confirm the foregoing by handwriting or in a similar form permitted by the applicable legal framework.
- to immediately cancel the authorizations to the information processes.

However, the Data Processor may keep a copy, with the data duly blocked, while liabilities regarding the service execution may arise.

Eleven. Audits

PROSEGUR may, within the scope of its inspection authority, conduct audits at its own expense to verify compliance with the information and personal data protection policies and security measures required by this Agreement. The audits may be conducted at the Data Processor's information systems and data processing facilities or by collecting information to confirm the Data Processor's compliance.

The Data Processor shall provide PROSEGUR with the documentation (in physical or electronic form) evidencing the performance of its obligations under the agreement.

Likewise, the Data Processor shall demonstrate that it has conducted the relevant risk analyzes and, if PROSEGUR so indicates, the relevant data protection impact assessments.

In order to facilitate or even avoid the verification by PROSEGUR, the Data Processor may provide the relevant certifications whose scope covers the services and employees it provides to PROSEGUR. If the Data Processor decides to make the above certifications, it must also provide the relevant documentation, certification, scope and reports of the audits to which it is subject pursuant to the certification. If, according to the risk analysis carried out by PROSEGUR,

PROSEGUR identifies security breaches incompatible with the provision of the Service, PROSEGUR may, depending on the severity, require the Data Processor to immediately remedy the problems identified by drawing up a detailed corrective action plan.

All of the foregoing is without prejudice to the possibility of conducting further audits or reviews to verify other obligations contained in this agreement.

Twelve. Duty of care

The Data Processor undertakes to provide the Controller with all information necessary to demonstrate compliance with its obligations and shall inform the Controller of compliance with any approved code of conduct or certification mechanism that may ensure compliance with its obligations in relation to the processing of Personal Data.

Individuals performing professional tasks for the Data Processor must be aware of the importance of PROSEGUR's information, handle it securely and be trained and qualified at each stage of the information processing for each of the functions they perform. They must exercise the utmost care and take appropriate measures to protect the processing of information in accordance with their duty of good faith, to which they are contractually bound.

Thirteen. Duty to inform

The personal data of the Data Processor's contacts will in turn be processed by PROSEGUR, located at Calle Pajaritos, 24, Madrid, in its capacity as Data Controller, in order to manage the relationship with the same in its capacity as Service Provider and on the basis of the execution of the Services. The data subject may exercise their rights of access, rectification, cancelation, opposition, restriction of treatment, portability and non-subjection to automated individual decisions by sending an email to the email address protecciondedatos@prosegur.com and attaching a copy of their ID card or equivalent document. The data subject also has the right to file a data protection complaint with the Spanish Data Protection Agency. Prosegur will handle them for the duration of the contractual relationship. Thereafter, they will be blocked during the limitation period of the applicable legal actions.

Fourteen. Artificial Intelligence

If the provision of services involves the use of Artificial Intelligence solutions by the Data Processor, the Data Processor warrants that the Artificial Intelligence solution complies with the principles and requirements set forth at **APPENDIX II** of this Agreement.

Likewise, the Data Processor guarantees compliance with the requirements required by the regulations applicable to the particular case.

The Data Processor shall take the necessary measures to ensure and demonstrate compliance with the obligations referred to in the preceding paragraph.

PROSEGUR may conduct audits within its control capabilities to verify compliance with the policies and measures required by this Agreement for the implementation of Artificial Intelligence Solutions. Processor agrees to participate in the evaluation process and implement the measures required by PROSEGUR to comply with its Responsible Artificial Intelligence Policy.

Fifteen. Compensation

The Data Processor agrees to indemnify Prosegur against any claims brought against Prosegur before the corresponding Supervisory Authority as a result of the Data Processor's and/or its subcontractors' failure to comply with the provisions of this Agreement and applicable personal data protection legislation, and agrees to pay the amount to which Prosegur may be ordered to pay in penalties, fines, compensation, damages and interest as a result of said failure, including attorneys' fees.

Sixteen. Jurisdiction

This agreement shall be governed by and construed in accordance with the laws of Spain, waiving any other jurisdiction that might correspond to them, and submitting to the exclusive jurisdiction of the courts and tribunals of the City of Madrid.

APPENDIX I. SECURITY MEASURES

In accordance with Articles 28 and 29 of GDPR, this section refers to the security measures that the Data Processor must adopt to ensure the level of security appropriate to the risk.

The Data Processor must implement the following technical and organizational security measures to ensure adequate security of Personal Data, including protection against unauthorized or unlawful processing and against loss, destruction or damage.

1. Organizational measures

The Data Processor is obliged to comply with the measures relating to the personnel who will have access to the Personal Data:

I. General organizational measures

1. The Data Processor shall ensure the existence and publication of an information security and data protection policy to ensure that the Processor has taken the necessary measures to ensure a level of security appropriate to the risk and that the protection of Personal Data is carried out in accordance with the applicable legislation.
2. The Data Processor must ensure that there is a structure (assigned department/role) responsible for information security and protection of personal data (internal data and external data of other customers).
3. Inventory of IT resources (servers, computers, software applications, backups) containing personal data.

II. Adherence to and compliance with PROSEGUR's Corporate Policies

1. The Data Processor shall comply with PROSEGUR's Information Security Policy (NG /GLO/ GR /04), the Document on Information Security Requirements for New Technology Projects (NE /GLO/ GR /SI/12) and the General Data Protection Policy (NG-GLO-LEG -12 - 3P), as amended from time to time. In this sense, the provisions of the aforementioned documents and all security measures defined or mentioned therein apply.

III. General measures related to personnel

1. The Data Processor must develop and implement an information security policy in accordance with security best practices, including obligations related to personnel.
2. The Data Processor shall ensure that the personnel assigned to the service have the appropriate skills and abilities to perform their duties.
3. The Data Processor shall ensure the development of a training and awareness program for suppliers, employees and third parties of the organization that process personal data. All users accessing personal data shall have received appropriate training in this regard for the functions to be performed.
4. Employment contracts should include specific clauses on compliance with the organization's security and privacy policies and should be signed by new employees before they are granted the right to access personal data processing assets, resources or facilities.

IV. Duty of confidentiality and secrecy

1. In order to prevent access to personal data by unauthorized persons, the Data Processor must ensure that measures are taken to prevent personal data from being disclosed to third parties (unattended electronic screens, printed documents left in publicly accessible areas, media containing personal data, etc.). This also applies to screens used to display images from the video surveillance system, if any. Personnel must lock the screen or end the active session when leaving their desk or workstation.
2. The Data Processor shall ensure that paper documents and electronic media are stored 24 hours a day in a secure location (cabinets or shelves with restricted access) and are under supervision when outside their respective storage facilities or archive rooms.
3. Printed (paper) or electronic (CD, USB stick, hard drive, etc.) documents containing personal data must not be discarded unless their destruction can be guaranteed, so that the information they contain is irretrievable.
4. Personal data or other personal information must not be disclosed to third parties, paying particular attention not to disclose protected personal data in telephone conversations, e-mails, etc.
5. The duty of confidentiality and non-disclosure shall continue even after termination of employment or provision of services.

V. Rights of the data subjects

1. The Data Processor must have a protocol for dealing with data subjects exercising their rights to ensure a prompt and effective response when exercising those rights.
2. The Data Processor must handle requests to exercise data protection rights, including but not limited to access, rectification and erasure.
3. The Data Processor must inform the Controller of such requests and assist the Controller in processing them.

VI. Personal data security breaches

1. The Data Processor must have a procedure for managing and reporting events (incidents, vulnerabilities, problems, etc.) under which events must be properly managed and reported to the Data Controller.

2. In the event of a personal data breach, such as theft or unauthorized access to personal data, the Data Controller shall be notified immediately of the breach, including all information necessary to clarify the facts and events that may have led to the unauthorized access to personal data. The Data Controller shall also be assisted in notifying the supervisory authority and, where applicable, the data subjects concerned, of the personal data breach, taking into account the information available from the Data Processor.

3. The Data Processor shall keep a log of all maintenance and/or support tasks of the Controller's systems.

2. Technical Measures.

I. Measures for physical and environmental access control.

1. Facilities should have perimeter security measures (walls, fences, access gates, barriers, video surveillance, on-site access authentication mechanisms, visitor reception, etc.) to protect information systems and personal data from unauthorized physical access and tampering.

2. Accesses to rooms and offices where personal data is processed must have technical and organizational measures to protect against unauthorized access (electronic access control, video surveillance, windows equipped with a system to detect breakage or tampering, procedures for requesting access to the room or office, personal identification, alarm system to detect intrusion).

3. Prior authorization should be required for the removal of storage media (hard drives, removable media, backup tapes) containing personal data from the premises.

4. Entrances and exits to and from secure areas of the facilities should be restricted and monitored by access control and video surveillance mechanisms to ensure that only authorized personnel have access to these areas.

5. The Data Processor shall ensure that technical and organizational measures are in place to protect data from immediate threats such as water leaks, data center fires, power outages, vandalism, etc.

II. Measures in connection with logical access control

1. The Data Processor shall define, document and establish a standardized account management procedure for access to information systems that process personal data [authorization request, creation, editing and deletion].

2. Access to personal data or systems processing personal data shall be granted only to users who have the appropriate authorizations (according to the defined process).

3. The Data Processor should document and implement a process to ensure that system access accounts are changed accordingly following organizational changes (e.g., function changes, terminations, layoffs, etc.).

4. The Data Processor must ensure that each user account is assigned a unique and unambiguous ID.

5. Changes to user accounts must be traceable (creation, editing, deletion) and evidence of this must be kept (e.g. in documents or records in information systems).

6. The Data Processor shall ensure that user authorizations are revoked immediately upon termination of the contractual relationship (including outsourcing).

7. Privileged access accounts for personal data processing systems should be reserved for authorized personnel only and limited in number.
8. Privileged accounts should only be granted to technically qualified personnel who have previously received special training and awareness on the management and use of privileged accounts.
9. Users who need to perform privileged activities involving personal information must have two accounts in the system: a standard account for performing routine tasks and operations, and a privileged account for performing tasks that require privileged privileges.
10. Default passwords for user accounts must meet the following complexity and security requirements:
    - They must be stored in encrypted form on information systems.
    - The passwords must not be displayed during password entry by the user.
    - The password must be changed after entering the original password to gain access to the system.
    - The maximum validity of the password must be ninety (90) days. The system will force the mandatory change of the password after the maximum validity period has expired.
    - The minimum length of the password must be eight (8) characters (including 2 numbers or special characters).
    - Password history must be at least three (3).
    - The number of consecutive unsuccessful attempts to enter the password before the account is locked must not exceed three (3).The password must have at least 8 characters).
    - The account must be automatically unlocked after at least 15 minutes if an incorrect password has been repeatedly entered.
    - Trivial or easy to guess passwords are to be prevented.
11. Control of access to data and information systems that process personal data should be based on a formally documented concept of roles and authorizations.
12. The assignment of authorizations/roles should be valid only for a limited time and should be made taking into account the principles of separation of duties (SoD) and the principle of least privilege.
13. The roles and permissions granted to the information systems used for the processing of personal data must be registered.
14. The authorizations granted should be reviewed regularly (at least once a year) to ensure compliance and validity.
15. There should be a clear policy of regular monitoring and dissemination among employees, which is part of the awareness-raising activities carried out by the organization.
16. The Data Processor's computers and workstations with access to information systems that process personal data shall have a password-protected screen saver that shall automatically activate after a period of inactivity not exceeding fifteen (15) minutes.

17. Employees and third parties using the Data Processor's computers and workstations should be encouraged to lock their screens when they leave their desks or workstations.

III. Measures to control transfer, storage and portability

1. All electronic transfers of personal data should be encrypted where appropriate.
2. Personal data processed by automated means should be stored in encrypted form where appropriate.
3. A record of personal data transfers via a physical medium [e.g., memory sticks, backup tapes, CDs, hard drives, etc.] should be formalized and retained.
4. Remote management of information systems that process personal data should be done through a secure communication channel (SSH, IPSec, TLS /SSL, VPN, etc.).
5. The Data Processor shall incorporate technical measures in the information systems to prevent the possibility of unauthorized export of personal data (e.g., restricting the functional features for downloading, printing, and storing data in information systems that process personal data).
6. The physical media used for the transfer of personal data should be encrypted.
7. Before disposing of computer media (USB, hard drives, etc.) on which sensitive personal data is processed, these media must be securely erased (so that the data is irretrievable).

IV. Security incident management control

1. Computers and peripheral devices (e.g., e-mail platforms, Internet access systems) must have an application to detect and protect against malicious software (e.g., viruses, Trojans, etc.), which should be updated regularly.
2. The Data Processor should have a security event management procedure that defines criteria for classifying, prioritizing, and escalating security incidents.
3. Processor shall periodically check the availability of security updates for IT systems and their components (including clients, network components, servers, etc.) that process Personal Data. Security updates are installed regularly as part of a formal process.
4. Information systems that process personal data should be scanned regularly for known vulnerabilities. Discovered vulnerabilities should be classified according to their criticality and impact on security and remediated accordingly.
5. The Data Processor should have a security event response team to respond to security events and help coordinate the resolution of security events.

V. Operational resilience control

1. The Data Processor should define, document and implement IT continuity plans covering critical IT systems and components.
2. The Data Processor should have intrusion and cyber attack detection and prevention tools (e.g., firewalls, IPS, IDS, targeted attack detection and prevention tools, etc.).
3. The Processor must have tools or services to detect and limit the impact of denial of service attacks (e.g., DoS, DDoS, etc.).

4. The Data Processor must regularly perform simulations of computer attacks (e.g., penetration testing). Detected deviations should be evaluated regularly and corrected according to a defined procedure.

5. Components and devices that process personal data must be protected against natural disasters (e.g., fires, floods, tornadoes, etc.) by appropriate technical and organizational measures.

6. The Data Processor's telecommunications networks should be segmented through the use of firewalls to limit the impact of a security event.

7. There is a backup policy for data processed by computer systems. The policy should specify the scope of IT systems, frequency of backups, retention period, physical location of backups, and security measures to protect confidentiality and integrity (e.g., encryption). The policy also considers regulatory and legal requirements.

8. Regular backups of computer systems (including system configuration data) that process personal data should be performed in accordance with the established policy.

VI. IT application development and operations control

1. The Data Processor should include security as an integrated element in the life cycle of its software development by adopting internationally recognized standards for secure application development. The Data Processor should identify and implement legal and security requirements in the early stages of development.

2. A log should be kept for users and administrators to the extent that activities are related to accessing the application (logging in, logging out, successful/failure attempts, etc.). Logging can at least identify who performed the action, when it was performed, and what type of action it was (e.g., logon, attempted access, etc.).

3. Log data should be stored securely and access to it should be limited to authorized personnel. Logs that must be retained due to their content and/or legal requirements should be deleted after their purpose has been fulfilled.

4. The Processor performs (static/dynamic) tests on the source code that it or a third party develops before deploying it in the production environment.

5. Non-production environments (e.g., development, testing, consolidation) should be completely separate from the production environment.

VII. Assurance and compliance control

1. The Data Processor shall regularly (at least once a year) and independently conduct security audits of the systems of IT that process personal data to ensure compliance with and effectiveness of the technical, organizational and legal controls in place. A record of the tests (and test results) must be maintained. Non-conformances are assessed, prioritized and corrected.

2. Regular simulations and tests of the established IT service continuity plans are performed (at least once a year). A record of the tests (and test results) must be maintained. Deviations shall be assessed, prioritized and corrected.

3. The Data Processor shall conduct periodic reviews (at least annually) of the security of the physical and environmental security controls in place to ensure their effectiveness. A record of the tests (and test results) must be maintained. Non-conformances are assessed, prioritized and corrected.

4. The Data Processor should periodically test the backups created and the recovery procedures established to ensure the integrity and availability of the backups. A record of the tests (and test results) must be maintained. Discrepancies should be assessed, prioritized, and corrected.
5. The Data Processor should periodically and independently review its information security management processes. The scope of the reviews should include, at a minimum, those controls that may impact the security of the data processor's personal data.
6. The Data Processor should have processes, operating procedures, and instructions in place to ensure compliance with legal, regulatory, and compliance requirements applicable to the type of service.

APPENDIX II. RESPONSIBLE ARTIFICIAL INTELLIGENCE

The artificial intelligence solution proposed by the SUPPLIER must comply with the following principles:

Respect for human autonomy

Respect for human freedom and autonomy must be ensured. The proposed AI system must be designed to enhance human cognitive, social, and cultural capabilities; human supervision and control of the proposed AI system's work processes must be ensured.

Principle of Prevention of Harm

It must be ensured that the AI system does not harm or otherwise affect humans and protects human dignity and physical and mental integrity.

The AI system and environment are safe and technically robust and must not be used for malicious purposes.

Special attention must also be paid to the potential adverse effects that an AI system could cause, and concrete mitigation measures must be defined to prevent possible harm.

Principle of Equity

It must ensure that the development, deployment, and use of the AI system are equitable by committing to ensuring a fair and equal distribution of benefits and costs and ensuring that individuals and groups are not subject to unfair prejudice, discrimination, or stigma.

The SUPPLIER will strive to prevent unfair bias and may identify specific measures to increase social equity through the use of AI systems.

Similarly, the use of the proposed AI system will respect the principle of fairness, i.e., the ability to appeal decisions made by the AI system and to communicate that appeal to those administering the system, and proportionality between means and ends, i.e., careful consideration will be given to how to balance various interests and competing goals.

Principle of Explainability

The explainability of the proposed AI system is due to the fact that all processes associated with AI development are transparent and clearly communicate the capabilities and purpose of the AI system to stakeholders.

Requirements for Responsible AI solutions

The following are the main requirements that must be ensured by the AI system solution to be a Responsible AI, which must be continuously assessed and addressed throughout the entire lifecycle of the AI systems:

Human Action and Oversight

AI systems should support people's autonomy and decision-making, supporting human action and promoting fundamental rights, as well as enabling human oversight.

The SUPPLIER ensures that automated decision making by AI systems requires as little human intervention as possible to ensure ethical, non-discriminatory decision making and to guarantee the rights and freedoms of individuals whose data are processed.

Technical Soundness and Safety

Technical soundness requires that the system IA be developed with a preventive approach to risk, so that it always behaves as expected and minimizes unintended and unforeseen harm, while also avoiding causing unacceptable harm, and that it ensures the physical and psychological integrity of people.

The SUPPLIER takes care that the system IA is robust and complies with the appropriate security measures to ensure the confidentiality, integrity and availability of the information stored and processed in it.

To this end, it conducts rigorous security tests and assessments to ensure that the IA system responds appropriately to security incidents that may result in the destruction, loss, accidental or unauthorized modification, or unauthorized disclosure of or access to such information.

Privacy and Data Management

The AI system takes care not to violate privacy, which requires proper data management, including data quality and integrity. Consequently, the AI system, its access protocol, and its ability to process data must be developed without violating privacy.

If the artificial intelligence solution provided by the SUPPLIER processes personal data, the SUPPLIER, as the controller of the AI system, adopts appropriate security measures of a legal, organizational and technical nature to ensure the protection of the freedoms and fundamental rights of data subjects, in strict compliance with the General Data Protection Regulation REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (hereinafter GDPR) and all applicable local regulations. It shall also ensure that only the data strictly necessary for each of the purposes envisaged are processed and that their retention is limited to the duration envisaged.

Transparency

For an AI system to be transparent it must have (i) traceability: the AI system's decisions are recorded in order to be able to identify the reasons for an erroneous decision by the system, which helps to prevent future errors, (ii) explainability: the decisions made by an AI system are understandable to humans and that they can track and (ii) communicate with them: that individuals are aware that they are interacting with an AI system and that the AI system should be identified as such and, where necessary,

the user should be given the possibility to decide whether he/she prefers to interact with an AI system or with another person, in order to ensure compliance with fundamental rights.

Diversity, Non-Discrimination and Equity

For a Responsible AI system to be reliable, it needs to ensure inclusion, diversity, equal access, through unique design processes, as well as equal treatment throughout its life cycle.

Furthermore, in the internal development and/or acquisition of AI solutions, the SUPPLIER guarantees in all cases the equality and non-discrimination of persons who may be affected by their use, in particular discrimination on the basis of race, color, ethnic or social origin, gender, sexual orientation, age, genetic characteristics, language, religion or belief, political opinion or otherwise.

Environmental and Social Well-Being

The SUPPLIER will promote sustainability and environmental responsibility through AI systems and advance research into AI solutions to address issues such as Sustainable Development.

Accountability

The SUPPLIER shall implement mechanisms to ensure responsibility and accountability for the IA system and its results, both before and after implementation.

In this regard, the SUPPLIER is accountable for the actions and decisions taken by an AI system, especially when progress is made towards autonomous systems capable of making automated decisions, and especially when these decisions have legal implications for the data subject.

7.5. ANNEX IV: Technological Risk and Cybersecurity Requirements

7.5.1. Technological Risk and Cybersecurity Requirements

7.5.1.1 Preliminary considerations

The processing of information and personal data under the responsibility of the Prosegur Group in the Supplier's premises is expressly authorized for the purposes stated in the agreement referred to in this annex. The removal of data carriers and documents containing information of Prosegur Group is expressly authorized, provided that this is necessary for the performance of the contracted services. In any case, when transferring data media and documents, the Supplier shall apply the security measures established to comply with this document or the applicable regulations.

The Supplier shall use the information and/or data resources in the possession of the Prosegur Group within the framework of the provision of the services entrusted to it and for the purpose previously specified.

7.5.1.1.1 Obligation to maintain confidentiality

All employees of the Supplier who have access to information related to the PROSEGUR GROUP as a result of the provision of the Service or for any other reason, shall keep it secret or confidential and shall not disclose it to any third party at any time, either before, during or after the provision of the Service.

The Supplier and its personnel may only use the information for the purpose intended in the subject matter of the agreement and shall be liable to the PROSEGUR GROUP for all damages incurred by the PROSEGUR GROUP as a result of non-compliance.

If the Supplier in turn subcontracts to a third party, the latter shall be responsible for respecting and complying with the same confidentiality criteria and rules regarding information related to the PROSEGUR GROUP as described in the previous clauses.

The Supplier, as well as its personnel involved in the provision of the service to the PROSEGUR GROUP, shall prevent any act or omission that could lead to unauthorized disclosure or misuse of the Data Assets involved in the development of the service.

7.5.1.1.2 Data confidentiality

The Supplier shall generally treat information from PROSEGUR GROUP as sensitive information and take the appropriate measures for such classification.

The processing of the information must enable traceability, i.e. it must be possible to identify which persons accessed and processed the information from PROSEGUR GROUP and when. Processing means any operation performed on the information, such as, but not limited to, reading, writing, modifying, copying, transmitting, recording or filing by manual means or by means of computer applications.

7.5.1.2 Compliance with legislation

The Supplier shall comply with all applicable laws affecting its scope relating to information security and privacy, as well as with the regulations of the industry for which Client provides the activity, and with regulatory, statutory and statutory requirements.

7.5.1.2.1 Personal data protection

The Supplier shall strictly comply with the provisions of the applicable legislation regarding personal data processed in the course of providing the Services covered by this Agreement.

The Supplier is obliged to keep the data absolutely confidential and in compliance with the instructions received from PROSEGUR GROUP regarding the purpose, content and use of the processing, applying data protection by default and by design and adopting the appropriate technical and organizational measures, and in particular with what is specified in the signed data protection agreements and commissioned processing agreements.

The Supplier shall conduct analyses of the legal and security risks for personal data and perform data protection impact assessments for those processing operations that are required under the provisions of the legislation in the relevant area of application.

7.5.1.3 Regulatory framework for information security

The Supplier shall establish an information technology security regulatory framework that ensures the proper implementation of the security measures specified in this Annex and that is consistent with the criteria of PROSEGUR GROUP regarding the security of the information handled.

The Supplier is obliged to update these security rules according to the changes of the Service and the new laws, regulations or standards with international reference and of countries that may arise in relation to technological security and protection of information and personal data, such as the NIST Cybersecurity Framework, the ISO 27000 and 22300 standards and/or other similar standards.

This regulatory framework must contain at least documentation related to:

- User management
- Access control and activity log management
- Personnel management
- Training and awareness-raising
- Incident management
- Service continuity management
- Operations management
- Information processing and destruction procedures

- Change management
- Software development and new system acquisitions
- Password policy
- Information disclosure and storage procedures
- Relationship and reporting model with PROSEGUR GROUP

Any of the specified documents may be requested from PROSEGUR GROUP to verify compliance with the minimum requirements and guarantees agreed with the supplier.

The Supplier shall warrant that the procedures for password assignment, distribution, and storage are in writing, with no exceptions not included in the above procedures.

The Supplier must communicate the legal framework to its employees entrusted with providing services to PROSEGUR GROUP and record their acceptance.

7.5.1.3.1 Risk management

The Supplier undertakes to carry out a risk analysis to determine the most appropriate technical and organizational measures to ensure and demonstrate that information is carried out in a responsible and secure manner, taking into account security aspects and the privacy and rights of data subjects. These measures shall have a preventive rather than a corrective approach and must be reviewed regularly to ensure that they are kept up to date.

The Supplier must conduct a risk analysis at regular intervals and in the event of relevant changes in the technological environment, taking into account in particular the risks associated with the service provided to PROSEGUR GROUP.

The Supplier must have a Risk Treatment Plan to address the risks identified in the analyses that need to be addressed. The effectiveness of the actions identified for risk treatment should be monitored.

7.5.1.3.2 Control schema

The Supplier agrees to comply with all policies, procedures and specific safety documents of PROSEGUR GROUP that are deemed applicable to the activities to be performed and that will be provided to the Supplier as soon as it begins providing the contracted services.

If the service involves information subject to security certifications, the Supplier shall provide PROSEGUR GROUP with the relevant certifications upon request.

The Supplier accepts and undertakes to comply with the control scheme applicable to the service provided, according to the classification resulting from the assessment carried out by PROSEGUR GROUP, the result of which will be made available to the Supplier.

The Supplier shall implement appropriate security controls to mitigate the risk of unauthorized access and modification of relevant information in the systems (applications, operating systems, and databases) supporting the Service and to prevent the loss, theft, unavailability, and unauthorized processing of information assets from the PROSEGUR GROUP.

The specified security requirements must be applied by Supplier. If the Supplier in turn subcontracts to a third party, it is itself responsible for ensuring that the security requirements are also met by that third party.

The PROSEGUR GROUP reserves the right to change the security requirements contained in this Agreement and its annexes at any time, and to notify Supplier with the effective date thereof.

7.5.1.4 Security organization

7.5.1.4.1 Identification of responsibilities

The Supplier shall have formally established technology risk Technological Risk and Information Security Managers, in order to ensure compliance with security policies and oversight of controls to ensure the integrity, confidentiality and availability, authenticity and traceability of data and systems, and compliance with all applicable regulations, with particular attention to those related to the protection of personal data.

The Technological Risks and Security Manager must assume control and coordination of the security measures applied by the Supplier, in particular those aimed at protection in the processing of personal data in the context of the provision of the service and carry out periodic audits to verify compliance with the aspects established in the Security Documentation.

The Supplier must designate a Coordinator responsible for managing the security aspects at PROSEGUR GROUP. This Coordinator of the Supplier must participate in the Coordination Committee formed by the Supplier and PROSEGUR GROUP, if the latter is convened by the PROSEGUR GROUP, in order to carry out a timely follow-up of the service and determine the necessary action plans to ensure the correct execution of the services.

The Supplier shall implement an appropriate segregation of duties by taking sufficient and necessary measures to ensure that access rights (roles and profiles) for each user of the service, are assigned according to the functional needs of each user and that these functional needs do not jeopardize the information assets that are part of the outsourced service.

The Supplier shall communicate the existence and persons performing the role of the Security Officer(s) and the DPO (Data Protection Officer) if they need or are required to do so in order to establish the appropriate communication.

The Supplier must communicate, through the channels established with the PROSEGUR GROUP, any change regarding the initial designation of the persons responsible for the Service, as well as communicate to the PROSEGUR GROUP, within a period not exceeding 24 hours, any termination of the User involved in the provision of the Service.

7.5.1.4.2 Training/awareness plans

The Supplier shall implement information security training and awareness plans that include all employees providing services to PROSEGUR GROUP.

The Supplier shall explicitly develop a plan to raise awareness of the importance of information security, personal data and its confidentiality.

The Supplier shall explicitly implement a training plan regarding the importance of developing secure code.

7.5.1.4.3 Notification

The Supplier must notify the PROSEGUR GROUP of any event that deviates from the contractual agreement reached with the PROSEGUR GROUP within a maximum period of 24 hours.

The Supplier must notify the PROSEGUR GROUP of any change arising during the provision of the service, either in the way it is provided (change in the process) or in the systems used to provide the service (change in the infrastructure), as well as the personnel involved in the same, within a maximum period of 24 hours.

7.5.1.5 Technological measures

7.5.1.5.1 Asset classification and management

The Supplier must have an inventory of information assets, indicating the type of information contained therein, the owner of the inventory, the custody and the degree of sensitivity of the information handled.

The Supplier shall establish a process for classifying information and categorizing assets and assigning them a security level commensurate with the inherent risks and criticality of the systems and information they support.

The Supplier shall maintain and update this inventory on a regular basis, in case of any change on the assets that are part of the service provision.

Data carriers shall be identified using a labeling system that is understandable only to authorized users.

The Supplier shall encrypt data when distributing media and portable devices and avoid processing on portable devices that do not allow encryption by taking measures to address risks in unprotected environments.

Ensure secure storage of data carriers containing PROSEGUR GROUP information in a location with restricted access to authorized personnel.

The Supplier shall implement sufficient mechanisms to ensure the secure storage of media containing PROSEGUR GROUP information when not stored in secure locations.

The Supplier shall have a Media Management Procedure that specifies methods for storing information media and who is responsible for authorizing access to such media.

Guarantee that any type of receipt or sending of media is performed only by authorized personnel, whether the recipient is a PROSEGUR GROUP company or an external company.

When documents contained in a file are transmitted, measures must be taken to prevent access to or manipulation of the information contained therein.

The supplier must keep records of incoming and outgoing data carriers that make it possible to identify the type of data carrier or document, the date and time, the sender and/or recipient, the type of information, the method of transmission and the person responsible.

The Supplier must take measures to prevent improper access to the information in the case of discarded data carriers.

7.5.1.5.2 Access control

The Supplier shall establish sufficient and necessary controls to ensure that physical and logical access to systems containing relevant information is controlled in accordance with the requirements established by the PROSEGUR GROUP in the regulatory framework specified in this Annex.

In granting access to the information, applications and systems involved in the Service, the Supplier shall use an identity management system based on roles and functions and taking into account the principle of “least privilege”, so as to ensure that its employees involved in the service provided to PROSEGUR GROUP are granted only the minimum level of access required for a given position.

The Supplier shall take sufficient and necessary measures to ensure that the access permissions and access controls configured in the systems involved in the service are regularly reviewed.

7.5.1.5.2.1 Control access to applications and systems

The Supplier must implement the necessary mechanisms to avoid the existence of generic users, except for those required by the technologies used. If required for the development of the service, these users must be approved and validated by the PROSEGUR GROUP.

The Supplier must implement the necessary mechanisms to uniquely identify its Users with access to the systems that are part of the service provided to the PROSEGUR GROUP. User codes and passwords may not be shared with other persons. The user codes used to access the applications must enable the Supplier to identify the accessing person unambiguously at any time.

The Supplier shall log the details of each access attempt, including information about the user, date and time, the file accessed, the type of access, and whether access was authorized or denied. If the access was approved, the access log is saved.

The Supplier must perform a periodic review of access control, reflecting the dates of valid or invalid access attempts. These records must be retained for a minimum of 2 years to search for evidence of security incidents.

The Supplier's Security Manager must have direct control over access to the access log control mechanisms.

The Supplier must implement the necessary mechanisms to have an updated user log. The Supplier must maintain an updated log for each system or application involved in the service provided to PROSEGUR GROUP. The log must reflect the association of each user code with its assigned person, profile and access permissions.

The log should reflect all changes in the mapping: additions, deletions and possible changes.

The Supplier must ensure that the user accounts of its users involved in the provision of the service that are found to be absent, or the accounts that are found to be inactive for more than sixty (60) days, must be deactivated. These user accounts may be reactivated if necessary, otherwise, if the inactivity continues for an extended period of time, these accounts will be permanently disabled.

The Supplier must ensure that its users involved in providing the service who change their work assignments shall have their access rights reviewed to determine if the assigned profile needs to be changed to ensure that they do not have access to information assets for which they do not have a valid business need.

The Supplier must implement the necessary mechanisms to allow for immediate processing of user cancelations. Cancelation of a user must be executed immediately through the application management tools, disabling access to the application with the canceled user code. The cancelation of a user means a temporary lockout before the final deletion takes place.

The Supplier must implement the necessary mechanisms to enable the availability of mechanisms for recording user activity.

The Supplier shall implement the necessary mechanisms to restrict access to the Internet or any type of connection that could allow the leakage of information about the data processed therein.

The Supplier shall define an access control/password policy that establishes a regulatory framework for access control based on the requirements of the service and Data Security.

The Supplier must implement these controls to ensure that all elements by which it delivers the service are securely managed and operated. These controls must be made available to PROSEGUR GROUP upon request.

The controls mentioned in the previous point should include:

- User/password policies for operators and system or product administrators, explicitly including database managers.
- Access to systems via tools that protect the confidentiality of administrator passwords, e.g. SSH in UNIX.
- Protecting server systems from unauthorized access.
- In case of access to confidential information, the Service must provide mechanisms for multi-level authentication.

The Supplier must consider at least the following aspects in its Password Policy:

- A password distribution procedure that ensures that passwords are known only to the user.
- A procedure to control the expiration of passwords and the incomprehensible storage of passwords.
- Appropriate robustness, to the extent possible in accordance with the following rules: (a) at least eight (8) characters in length, (b) uppercase letters, (c) lowercase letters, ¡d) numbers, and (e) special characters (e.g. !, $, @)
- Password expiration (recommended 60 days and no more than 90 days), with a change procedure that does not cause an interruption of service.
- Mandatory encrypted storage of passwords for the systems and applications that are part of the outsourcing.

The Supplier shall implement the necessary mechanisms to grant access rights to the systems providing services to the PROSEGUR GROUP only to the personnel authorized in the Security Document and in the user lists of each system.

The Supplier shall implement a mechanism to limit the number of repeated attempts of unauthorized access.

The Supplier shall establish sufficient and necessary controls to ensure that logical access to systems holding relevant information is controlled in accordance with the requirements established by the PROSEGUR GROUP.

The Supplier must ensure that employees who need to use remote connections to provide the service comply with the guidelines of the Prosegur Group Remote Access rules provided for the provision of the service as soon as the relevant and contractually agreed activities are commenced. In particular, that:

- All remote access must be approved in advance by the PROSEGUR GROUP.
- The access data must have a unique identifier assigned to a user and must not be transferable.
- In the event that an employee shares their credentials or shares their open session with other users:
    - This will be considered as a security incident.
    - The user will be immediately removed from the systems of the PROSEGUR GROUP.
    - The employee, and therefore the Supplier, shall be directly responsible for the actions (or omissions) of the user representing it and may be subject to the penalties provided in the event of misuse.

The Supplier shall establish mechanisms to identify access to documents to which multiple users have access.

The Supplier shall take sufficient and necessary measures to ensure regular review of access permissions and access controls in the systems involved in the Service.

The Supplier must take sufficient and necessary measures to ensure that remote access to the technical environment is controlled and monitored.

The Supplier must ensure that the information related to the provided Service is not disclosed to third parties without prior authorization from PROSEGUR GROUP and within the legal framework.

7.5.1.5.2.2 Control access to facilities and DPC

The Supplier must ensure access control to the rooms where the assets involved in the service provided to the PROSEGUR GROUP are located, with the appropriate administrative, logical and physical safeguards, including depending on the criticality of the systems, but not limited to:

- Locking of access doors

- Secure destruction of information assets, in a timely manner.
- Access to the Supplier's offices and data processing centers;
- Secure storage devices;
- Physical security personnel
- Video monitored areas

The Supplier shall ensure that unauthorized entry is prevented, detected and reported immediately to the appropriate Supplier personnel. All entrances and exits must be secured, logged and monitored to ensure that only authorized personnel can enter Supplier's buildings and secure areas.

If the Supplier uses identification cards or similar tokens for its employees that are part of the service provided to the PROSEGUR GROUP, there shall be a documented process and supporting procedures to ensure that lost credentials and tokens are deactivated immediately upon notification of the loss.

The Supplier must have sufficient procedures and mechanisms in place to ensure that in the event of termination of employment of an employee who is part of the service provided to the PROSEGUR GROUP, the identification credentials are immediately deactivated.

The Supplier must ensure that all PROSEGUR GROUP information assets that are part of the outsourced service, in the possession of the Supplier, are physically secured in an access controlled area, locked room, or secure storage container or filing cabinet.

The Supplier shall notify the PROSEGUR GROUP of any relocation or removal of information systems or assets that may not be performed without the written consent of the PROSEGUR GROUP.

7.5.1.5.2.3 Physical and environmental controls

The Supplier shall be responsible for implementing physical security measures to protect information systems located in its facilities from unauthorized access and physical damage.

Physical and environmental controls should include the following:

- Fire protection measures
- Flood protection measures
- Control of energy supply
- Other controls applicable according to laws and regulations.

The Supplier shall establish sufficient and necessary controls to ensure that physical access to the premises where the information systems containing the relevant information are located is maintained. In addition, the database of personnel authorized to access must be updated and controlled in accordance with the requirements established by the PROSEGUR GROUP.

7.5.1.5.2.4 Authorization and authentication

The Supplier shall take necessary and sufficient security measures to ensure that administrator access to information systems is through encrypted channels and strong authentication.

If the Service requires servicing customers, the Supplier must implement the necessary and sufficient security measures to ensure that those customers are authenticated with two-factor mechanisms, at least for performing operations or requesting confidential information.

The Supplier must guarantee the encrypted storage of passwords in the information processing systems.

The Supplier must implement the necessary mechanisms to uniquely identify the accesses of each user and only allow access to the data and resources necessary for the development of their functions.

The Supplier must implement the necessary mechanisms to prevent users from being local administrators of their posts, unless this is expressly requested and confirmed by the PROSEGUR GROUP.

7.5.1.5.3 Encryption

The Supplier shall use standard encryption algorithms with a key length based on internationally accepted practices and standards to protect the confidentiality and integrity of THE PROSEGUR GROUP 's sensitive data.

The Supplier shall protect the encryption keys with security mechanisms throughout their life cycle, from their generation to their storage, distribution, renewal, archiving and disposal.

The Supplier shall provide the PROSEGUR GROUP with documentation of encryption key management to verify that minimum security requirements for cryptographic keys are met. If access to Prosegur GROUP systems is required, the rules and procedures that the Supplier and its personnel need to know regarding encryption key management and use shall be provided at the time of commencement of operations.

The Supplier shall ensure that devices on which critical or sensitive data is processed are encrypted. This applies in particular to mobile devices such as laptops or removable media.

Loss of confidentiality of a cryptographic key affecting Prosegur Group systems is a security incident and must be reported immediately so that the appropriate mechanisms can be initiated.

7.5.1.5.4 Perimeter and infrastructure security

The Supplier shall inform the PROSEGUR GROUP about the technological infrastructure deployed to provide the Service, with the level of detail required by the PROSEGUR GROUP to allow performing the supervision/monitoring tasks established by the PROSEGUR GROUP.

The Supplier must develop a technological infrastructure for the provision of the service, so as to facilitate the modular migration to another location or a technology migration.

The Supplier must not connect neither hardware nor software not owned by the PROSEGUR GROUP to the internal network of the PROSEGUR GROUP without:

- A risk assessment with the necessary scope, including identification of existing and compensating controls based on the requirements within this annex;
- Review of the implementation of controls identified in the risk assessment;
- Written approval by the Client's Chief Security Officer (CISO).

The Supplier shall secure or disable unattended network ports when not in use. If business needs warrant the need to enable them, network ports may remain active as long as the Supplier's management has reviewed the business need and documented approval has been obtained. Examples of such a need would be network ports in conference rooms, shared work areas, etc.

7.5.1.5.4.1 Separation of environments (if the Supplier manages the infrastructure for providing the Service)

The Supplier's production environment must be physically or logically separated from the non-production environments so that the exchange of information between them is controlled.

The Supplier's user network must be separate from the central system network and provide a minimum level of connectivity necessary for users to access the systems they need to perform their tasks.

In all cases, segmentation into operational, development, and test environments must be established to reduce the risks of unauthorized access or modification and to avoid impacting production systems.

7.5.1.5.4.2 Server Security (If the Supplier manages the infrastructure for providing the Service)

The Supplier must have documentation or guides for server bastioning, patch management, versions, and vulnerabilities that ensure the security of the systems and their availability. Servers must have only the software necessary to properly provide the service installed and have up-to-date virus protection.

The servers must be set up in accordance with recognized good practices and must have only the necessary services enabled.

The servers required to provide the service should, if possible, be logically segmented, for example by reserving a VLAN for the service provided to the PROSEGUR GROUP.

Protection of the data must be ensured and ensure that it is only visible to the PROSEGUR GROUP. The data, whether stored in databases or file systems, is only accessible from the applications that process it and should never be publicly accessible from external networks.

The database server must be installed on a different system than the application's execution system and must only allow communication with the server hosting the application, i.e. it must not be directly accessible via the Internet.

The servers must be properly locked/sealed so that any tampering can be visually detected.

7.5.1.5.4.3 Perimeter security

The server hosting the application must be protected from third-party access by a firewall.

If there are applications exposed to the Internet, access to them must be shielded by a device that works as a reverse proxy and is located in a DMZ protected by a double firewall barrier. There should be no direct access to the Internet unless the PROSEGUR GROUP explicitly allows it.

The Supplier shall ensure that, in the event new software is integrated onto devices with connectivity privileges to PROSEGUR GROUP's information systems, it is preceded by a risk assessment and formal change control procedures are implemented to determine and protect the impact on PROSEGUR GROUP's network.

7.5.1.5.4.4 Wireless network

The Supplier shall configure wireless network access points so that only Supplier-authorized devices can connect to Supplier's internal network where PROSEGUR GROUP information is viewed, hosted, stored, processed, transmitted, printed, secured, or destroyed. In addition, the wireless network connections established shall use industry standard encryption practices and other appropriate safeguards to protect against unauthorized access and use.

7.5.1.5.4.5 Endpoint Security

The Supplier must implement an endpoint protection solution that includes:

- Anti-malware applications as part of standard secure configurations for systems, devices and components. Vulnerability detection and updates, user modification prevention, and frequent scans.
- Personal firewalls with port and service restrictions, control against running malware, control of removable media such as USB devices, and audit and logging capabilities.
- IDPS tools to detect and stop suspicious activity by monitoring network traffic and the devices that connect to it.
- Restrictions on the use of mobile code to prevent malicious code from running on computers.

7.5.1.5.5 Personnel management

The supplier must implement human resource management procedures for the hiring, retention, and dismissal of employees, contractors and other personnel working on behalf of the organization.

The supplier must agree to apply appropriate selection criteria for positions involving PROSEGUR GROUP systems.

The Supplier must ensure that human resource management is linked to risk management. Therefore, it must ensure that there are processes in place for registering, changing, and terminating staff that specify that if there is a change in their situation, the appropriate action will be taken immediately, such as removal from systems or revocation of access privileges, to ensure the security of information and systems.

The Supplier shall ensure that its personnel and/or its subcontractors' personnel and/or its subcontractors' personnel who are to have access to the Prosegur Group's systems, assets and information are aware of and comply with the policies, rules and procedures provided by the Prosegur

Group once the Agreement has been formalized and the services have commenced, in particular with regard to their duties and obligations concerning the use of the Prosegur Group's systems, networks and other resources, as well as the consequences and sanctions for non-compliance.

In particular, the Supplier must ensure that its employees do not take any action except with the written authorization of Prosegur:

- Install any software or equipment in the Prosegur environment that has not been approved by Prosegur.
- Upload obscene, offensive or inappropriate data or software that violates Prosegur's licensing policy in the Prosegur environment.
- Use the Prosegur environment to intercept, analyze or otherwise monitor traffic on the Prosegur networks.

The Supplier shall provide adequate cybersecurity and data protection training and awareness to its employees by having Training and Awareness plans for personnel that are managed between the risk management team and HR. The Prosegur Group may request to see the content of the staff training and awareness plans in order to verify their adequacy.

The supplier must ensure that privileged users with specific security roles receive specific training to ensure they understand their specific roles and responsibilities.

The supplier must ensure that outsourced personnel meet the same training and awareness requirements as other personnel.

7.5.1.5.6 Operations management

The Supplier must establish appropriate security controls to ensure that operations performed on applications and systems involved in the service are authorized and scheduled in accordance with requirements agreed upon between the PROSEGUR GROUP and the Supplier. Specifically, the operations to be considered in the service refer to the generation of backup copies and the management of technological security incidents.

The Supplier must have a set of policies defining the measures to be taken for the creation of backup copies and the procedures to be followed for the recovery of the systems.

The Supplier must have established a set of measures specifying the actions to be taken for the proper management (detection, resolution and notification to the PROSEGUR GROUP) of the technical security incidents that occur during the provision of the service.

7.5.1.5.6.1 Configuration of the systems

The Supplier must ensure that there are processes for the configuration management and bastioning of the systems that comply with the international standards and that allow the application of the security requirements established by the PROSEGUR GROUP for the systems.

Configuration management must be centralized for all operating systems, applications, servers and other technologies that can be configured.

The supplier must keep a record of historical configurations if required for troubleshooting or forensic purposes.

Identified unauthorized configuration changes that impact the PROSEGUR GROUP assets must be treated as security incidents and reported to PROSEGUR GROUP.

The Supplier must install anti-virus protection on the systems used to provide the service to the PROSEGUR GROUP, which must be kept operational and up to date at all times.

The Supplier must implement controls to restrict output devices such as USB, CD /DVD reader/writer or others that allow extraction of data.

7.5.1.5.6.2 Systems maintenance (in case the Supplier uses its own systems to provide the Service to the PROSEGUR GROUP).

The Supplier must implement a vulnerability monitoring process for the technical infrastructure of the Service to detect and address vulnerabilities in a timely manner without exposing PROSEGUR GROUP's data to such risks. In addition, it must periodically conduct a security assessment of the internal network and the perimeter network, either with its own resources or through an independent third party.

The Supplier may proactively suggest the installation of security updates and patches. Such updates and patches will be communicated and approved by the PROSEGUR GROUP. In addition, the PROSEGUR GROUP will request the installation of updates and patches when deemed necessary.

In any case, the installation of patches must be tested in previous environments to avoid any possible impact on the Service.

Regardless of the base software supporting the platform and its versions (operating systems, database, web server, etc.), there must be a policy for monitoring security alerts and updating security patches released by the appropriate vendors.

In case of security flaws that are classified as serious/high by the manufacturer, the response time should not exceed 24 hours.

The Supplier must establish appropriate security controls related to changes that must be made to applications or systems involved in the service. At a minimum, these controls shall include change requests, impact analysis, authorizations, testing, end user approvals, and appropriate separation of upstream environments from the production environment.

Implementation of changes to information systems associated with the Service must be approved in advance by the PROSEGUR GROUP and must ensure the integrity, confidentiality, and availability of the information and the Service.

The Supplier shall establish the necessary mechanisms for the management and operation of the security arrangements, provided that the PROSEGUR GROUP makes an explicit delegation of these functions.

7.5.1.5.6.3 Location of the data (in case the Supplier needs to store information related to the provision of the Service to PROSEGUR GROUP in its own systems).

The Supplier must inform the PROSEGUR GROUP of the location of the data to be stored prior to engaging the Service. During the term of the Service, any change in the location of the data must be notified to the PROSEGUR GROUP in advance and the changes can be made only after approval by PROSEGUR GROUP.

The Supplier must implement change control mechanisms in the files stored in the Service and record all the necessary information that allows the traceability of the events.

7.5.1.5.6.4 Temporary files

The Supplier shall, in the case of the use of temporary files or auxiliary files for the provision of the service, protect such files with the same security measures used for the main files and securely delete, remove or destroy them as soon as they are no longer necessary for the purposes for which they were created and ensure that their subsequent recovery is not possible.

The persons in charge of the information systems designated for this purpose shall periodically verify the possible existence of temporary files created automatically due to malfunctions of the systems.

Unless required by the service, the printing of personal data from the management applications on paper shall be avoided.

7.5.1.5.6.5 Shared service

The Supplier must take sufficient measures to ensure the security of the technological infrastructure if it is shared with other customers of the Supplier. The technological infrastructure of the Service must have encrypted communication channels between other services offered by the Supplier and the connections of the personnel responsible for managing the infrastructure. For example: SSH, VPN with IPSEC, etc.

The data storage of the Service provided to the PROSEGUR GROUP must be logically isolated from other external storage systems. The Supplier's service must be able to encrypt stored information, using strong encryption algorithms as needed.

7.5.1.5.7 Incident management

The Supplier shall have a security and privacy incident management and reporting procedure and shall notify PROSEGUR GROUP in a timely manner of a potential security incident or the occurrence of a security incident and its resolution. This procedure must be brought to the attention and awareness of all employees.

With respect to incident management, the Supplier shall have automated and management mechanisms that cover the following:

- Prevention

- Detection
- Analysis
- Containment
- Mitigation
- Recovery
- Monitoring

The Supplier must take the appropriate measures to ensure that the anomaly that led to the incident is corrected as soon as possible.

The Supplier must record the following for each incident that occurred: type of incident, description, time of occurrence or discovery, person reporting the incident, person notified of the incident, inferred impact, corrective actions applied, data recovery procedures performed, person performing them, data recovered, and data manually recorded.

The Supplier must approve the execution of data recovery procedures (if required) according to the recovery plans available to it.

The Supplier shall provide the PROSEGUR GROUP with the necessary support if it decides to initiate an independent security assessment or investigation of the incident.

The Supplier must define a secure means of communication to communicate unusual situations, incidents or other types of information concerning the confidentiality of the PROSEGUR GROUP without unnecessary delay.

The Supplier shall immediately notify the PROSEGUR GROUP when a security incident is discovered or suspected and provide a report with information about the incident, the processes, assets and information affected, the actions taken and their resolution. The PROSEGUR GROUP may follow up on these incidents to identify potential situations where specific actions should be taken.

The Supplier shall agree with the PROSEGUR GROUP the criteria for reporting a security incident in cases of information loss, service interruption, attacks affecting the reputation of the PROSEGUR GROUP and any other agreed case.

Failure to report a critical incident of which it has become aware may be considered a breach of processing security and constitute a breach of good faith.

The Supplier shall maintain a security incident log, at a minimum, for the systems and facilities that affect the PROSEGUR GROUP. This shall include the incidents that occurred, the impact, the dates and times of discovery and remediation of the incident, the individuals who were responsible for managing the incident, and the solutions and actions implemented to remediate the incident.

The PROSEGUR GROUP may inspect the list of incidents affecting its systems and assets or request a report on the monitoring of events and incidents affecting its systems and information at any time, if required. The Supplier must be able to produce it.

7.5.1.5.8 Communications

The Supplier shall establish all necessary mechanisms to ensure that communications over public networks or wireless electronic communications networks are encrypted.

The Supplier's DPC can be connected to the systems of the PROSEGUR GROUP only if the control measures established by the PROSEGUR GROUP are set up after a detailed analysis of the need.

Communication with the DPC of the PROSEGUR GROUP must be redundant.

The Supplier must provide PROSEGUR GROUP, upon request, with a complete map of the Service Provider's network, detailing all the communication elements involved, as well as the security elements.

At a minimum, the Supplier shall have the following perimeter security measures in place: Firewall, Intrusion Detection and Prevention Systems (IDS /IDPS), Demilitarized Zone (DMZ), Virtual Private Networks (VPN) and Proxy.

7.5.1.5.8.1 Security in the use of electronic mail (in case the Supplier sends mail on behalf of the PROSEGUR GROUP or with information relating to it)

If the Supplier sends mailings on behalf of PROSEGUR GROUP or with information that relates to, Supplier must comply with the following measures:

- The web addresses (URLs) contained in the mailings and their content must be reviewed in advance by the PROSEGUR GROUP Information Security Department.
- The Information Security Department of the PROSEGUR GROUP must know the PROSEGUR GROUP data to be included in the emails. These should not be confidential or secret, and this department will decide if and how they need to be secured.
- The PROSEGUR GROUP's Information Security must receive:
    - Prior notice of the sending of emails.
    - A brief explanation of the content of the email.
    - An example of the email/SMS that customers will receive.
    - Information on the mailbox of origin of the email that customers will receive.
- There must be traces and evidence (logs) of when and to whom the emails are sent from the mail server used to send the emails, regardless of whether this is done in the infrastructure of the PROSEGUR GROUP or in the infrastructure of the Supplier.
- The activity records (logs) must record the date and time of sending, the account from which the email is sent and the recipients of the email.
- The emails must contain the warnings/recommendations agreed upon with the Technology Fraud Control Department.

- The emails must be sent with a domain registered in the name of the PROSEGUR GROUP.
- The messaging department (if PROSEGUR GROUP sends the email) or the Service Provider must set up control mechanisms via the SPAM blacklists to control that PROSEGUR GROUP domains do not show up.
- Emails sent to customers must go through the necessary checks to be free of viruses. This means that the emails must be scanned using existing antivirus tools at PROSEGUR GROUP or, in the case of outsourcing, at the Service Provider.

7.5.1.5.9 Capacity management, sizing and systems procurement

The Supplier must manage the capacity and resources that affect the service provided by establishing capacity management and sizing processes consisting of dynamic management of the Supplier's resources based on demand, contractual obligations and economic capacity.

Acquisition of new systems, equipment, components, or software should be made with these factors in mind:

- The risks associated with each activity, service, and system.
- They must be consistent with the requirements and security architecture of the service.
- The technical requirements for the resources
- The effort and economic means for implementation.

The Supplier must establish appropriate security controls with respect to the acquisition and development of new applications and/or new systems, and with respect to changes that must be made to applications or systems affected by outsourcing during the performance of the service. These controls should include, at a minimum, authorization, testing, end user approvals, and appropriate separation of upstream environments from the production environment.

7.5.1.5.9.1 Use and development of software for the provision of the service

The Supplier must use only software licensed and tested by the PROSEGUR GROUP and the Supplier, for the development of the outsourced service.

All developments made with the purpose of providing services to PROSEGUR GROUP must be approved by the PROSEGUR GROUP, and the Supplier must:

- Refrain from storing PROSEGUR GROUP data without the knowledge, approval and/or testing of PROSEGUR GROUP.
- Perform a security review of the source code for any software not developed by PROSEGUR GROUP before it goes into production, in accordance with the principles and good practices of secure development.

- If software developments are made for PROSEGUR GROUP, Supplier shall provide PROSEGUR GROUP with all such custom software developments, including source code, object code, manuals and any other relevant information.

- Be available to perform a control environment assessment, ethical hacking, or other security assessment before releasing a version of the system to production whenever requested by the PROSEGUR GROUP.

- Non-production environments must not contain real data and must have the same controls as the production environment.

- Ensure that developments made to provide the Services to the PROSEGUR GROUP and the tools used comply with intellectual property laws and do not violate any laws, regulations, agreements, rights, interests or property of third parties.

- Establish appropriate security controls with respect to the acquisition or development of new applications or systems during the provision of the Service. At a minimum, these controls should include feasibility analysis, approvals, testing, end-user approvals, and adequate separation of upstream environments from the production environment.

- The Supplier must follow the best practices of secure software development in accordance with the requirements of the standard and avoid the introduction of known vulnerabilities if software is developed.

- PROSEGUR GROUP development teams shall be located in network segments and environments dedicated solely to application development, without access to production environments or actual PROSEGUR GROUP data.

- The Supplier shall establish appropriate security controls related to integrity validation of developments in production environments.

7.5.1.5.10 Review

7.5.1.5.10.1 Reviews conducted by the PROSEGUR GROUP.

The Supplier accepts the performance of reviews of compliance with the control scheme by the PROSEGUR GROUP, on the following basis:

- Ordinary, as part of the evaluation of the provision of the Service.

- Extraordinary, due to a security incident or in the event of an extension, regression of the Services or due to circumstances that lead PROSEGUR GROUP to deem it appropriate to conduct these reviews.

The PROSEGUR GROUP will conduct these reviews according to the control scheme, following an evaluation method, scope, follow-up method and periodicity set by the PROSEGUR GROUP.

The Supplier shall cooperate as necessary to meet the requirements of the review, which may be formulated by PROSEGUR GROUP, the persons or companies designated by PROSEGUR GROUP, and provide them with any documentation and/or evidence requested for the purposes of this review.

In addition, PROSEGUR GROUP may exercise control over the technological risks associated with the Service, and the Supplier is responsible for providing the following information when required:

- Review of audit reports and/or certifications, for example:
    - Internal Audit/Internal Control reports.
    - Independent third party reports (SOC 2 Type 2, ISAE 3402, SSAE 16, etc.).
    - Security certifications (ISO 27001, 22301, etc.).
    - Service quality certifications (ISO 9001, ISO 2000, etc.).

In addition to the reports submitted, the PROSEGUR GROUP must be able to develop a plan for evaluating technology risk controls and execute it in accordance with schedules, scopes, and procedures to be agreed upon with the Supplier. This plan may include:

- Regular monitoring of service safety indicators:
    - The indicators to be monitored were agreed upon prior to the signing of the agreement and should be reviewed on a regular basis.
    - Access to dashboards or consoles by the PROSEGUR GROUP, allowing continuous monitoring of technological risk.
- Reporting of relevant events by the Supplier:
    - Security incidents.
    - Disaster recovery testing.
- Information about the technological infrastructure that supports the PROSEGUR GROUP (in case the Supplier uses its own infrastructure for the provision of the Service):
    - Network architecture.
    - Perimeter security architecture.
    - Servers and databases.
    - Network and communications protocols.
    - Others necessary for the PROSEGUR GROUP to adequately perform its control functions.
- Information on the monitoring of the systems serving the PROSEGUR GROUP and the relationship model established for the transmission of this information, if deemed necessary.

The Supplier shall address control weaknesses identified by PROSEGUR GROUP in reviews conducted in accordance with agreed upon action plans.

7.5.1.5.10.2 Supplier's internal control

The Supplier shall have an internal control function to ensure compliance with all controls required by the PROSEGUR GROUP.

The Supplier shall describe the procedures and controls it will implement internally to ensure that the above requirements are met and make them available upon request to PROSEGUR GROUP.

The Supplier shall conduct all legally required internal and external audits of the systems involved in the service provided to the PROSEGUR GROUP, and make the audit reports generated available to PROSEGUR GROUP.

The Supplier shall conduct a security review of its systems when significant changes are made to the information systems. It shall provide PROSEGUR GROUP with the report of this review and propose corrective actions.

7.5.1.5.10.3 Coordinated controls with the PROSEGUR GROUP.

The PROSEGUR GROUP and the Supplier will agree to procedures for diligent notification of security incidents to PROSEGUR GROUP. Specific communication protocols will be established for instances where the PROSEGUR GROUP needs to take immediate action to mitigate the impact of security incidents.

PROSEGUR GROUP may at any time satisfy itself of compliance with the technical requirements, both by visiting the Supplier's facilities and by using secure means of remote access to the affected systems, as agreed with the Supplier.

Those aspects observed during these verifications that PROSEGUR GROUP considers to be in breach of the present provisions or that could compromise the systems of PROSEGUR GROUP will be reported to the Supplier, who will be given a deadline to remedy them, with the consequent contractual obligation that the Supplier complies with the observed aspects as agreed with the PROSEGUR GROUP.

7.5.1.5.10.4 Return of Service

The PROSEGUR GROUP and the Supplier must define and agree upon procedures for the return of the Service that ensure secure storage of media and, if applicable, secure destruction of information used by the Supplier during the provision of the Service.

The Supplier shall ensure that secure mechanisms are used to destroy information. This also applies to cases of media recycling and termination of Service.

If the destruction of information is carried out by a third party, the PROSEGUR GROUP must be informed about it and receive a certificate of secure destruction.

The Supplier shall comply with the guidelines provided in the applicable international standards and practices in the aspects applicable to the outsourced service.

Retention periods must be established and properly maintained by the Supplier for records that comply with legal retention requirements. In addition, the PROSEGUR GROUP may provide for specific retention requirements that Supplier will apply, including but not limited to, retention for litigation, legal or regulatory purposes.

Supplier shall ensure that the destruction of the PROSEGUR GROUP systems and assets that are part of the Service is in accordance with the Supplier's records management program. Before a workstation or server is reused, decommissioned, or returned to the leasing provider, destruction methods must be performed in a secure manner so that the information cannot be read or recreated after disposal.

The Supplier must take into account the impact of disposal on the environment.

7.5.1.5.11 Monitoring

The Supplier shall make available to PROSEGUR GROUP, upon request, the procedures and controls it will use to monitor and warn of potential breaches in the security of the systems.

The Supplier shall establish the necessary mechanisms to monitor the software installed on the equipment providing services to the PROSEGUR GROUP so that only the software that is essential for the proper provision of the service can be installed, regardless of whether the systems are owned by the user or by the PROSEGUR GROUP.

7.5.1.5.11.1 Retention and use of security logs.

Regarding the events that generate logs, the format and content of the logs, as well as the retention period, will be established by the PROSEGUR GROUP. Upon request, these logs must be available in real time, either by direct access to the provider's system or by receipt in the internal repositories of the PROSEGUR GROUP. In addition, it must be verified that traceability is guaranteed in the other systems indirectly involved in the service or previously analyzed by the PROSEGUR GROUP. The Supplier must generate logs (access, authentication, administration and activity), at a minimum, of the following events:

- Communications.
- Sending files (systems involved in the transmission, both at origin and destination, and intermediate temporary storage systems).
- Web applications.
- Virtualization systems (client-server architecture).
- Backend (servers and applications).

7.5.1.5.12 Back-up and recovery copies (in case the Prosegur Group authorizes the backup of the data or systems for the provision of the Service to the PROSEGUR GROUP)

The Supplier shall establish and implement a backup policy that includes backup security, testing and recovery procedures. It shall have controls in place to ensure proper handling and transportation of backup media, assignment of responsible parties, physical and logical access controls, chain of custody, and periodic inventories, and to ensure the confidentiality of the information contained therein.

The Supplier shall implement controls in its backup policy to ensure the restoration of data to the condition it was in at the time of modification, loss or destruction.

The Supplier shall establish procedures for at least weekly backups, unless no update of the data has occurred during that period.

The Supplier shall regularly back up its systems in accordance with the recovery time and recovery point objectives to be included in the Business Continuity and Disaster Recovery Plan and agreed with PROSEGUR GROUP.

The Supplier must house both the backup and recovery procedures and the copies themselves in a location other than the Information Systems.

The Supplier shall maintain a maximum of one (1) full and incremental backup copy of the following six (6) days at its own facilities, any copies not within this range shall be off-site.

The Supplier backup policy shall include semi-annual review and testing of the effectiveness of the copying procedures by the Data Controller.

Work will only be done with real data if the security level corresponding to the processing is guaranteed.

Copies shall be made or documents reproduced only under the control of the personnel specified in the security document, and discarded copies shall be destroyed in such a way that their information is inaccessible.

7.5.1.5.13 Business continuity

The Supplier shall have a Business Continuity and Disaster Recovery Plan in place to recover information systems, formally document and regularly test service, and ensure availability of service provided to the PROSEGUR GROUP.

The Supplier shall review the Continuity Plans at least annually and whenever there is a relevant technological, organizational or regulatory change.

The Supplier shall ensure that all personnel assigned to business continuity tasks have sufficient experience, competence and capacity to perform the required functions.

The Supplier must conduct contingency testing to demonstrate the effectiveness of continuity and disaster recovery plans. Likewise, it must be part of the testing required by PROSEGUR GROUP as part of the Continuity of PROSEGUR GROUP's systems.

The Supplier must regularly inform the PROSEGUR GROUP about the status of the continuity of the service provided, in accordance with the instructions provided.

In the event of an interruption due to a security event, the Supplier shall assume responsibility for resuming the services provided within the deadlines set by the PROSEGUR GROUP, depending on the criticality of the affected systems. For systems with higher criticality, resumption of activities may be required within 4 hours. The Supplier is responsible for resuming the services within the agreed deadlines and unjustified non-compliance may result in contractual consequences and penalties.

The Supplier shall allow PROSEGUR GROUP to conduct audits of the Supplier's Business Continuity Plan (BCP) and Disaster Recovery Plan (DR) related to or affecting the information assets included in

the outsourced service, including BCP and DR procedures and the results of tests performed, at least once a year and after any contingency or natural disaster.

7.5.1.5.14 Supplier management

The Supplier must ensure that mechanisms are in place to manage third parties when the services it provides depend on other suppliers.

The Supplier shall ensure that its risk management team can implement coordinated actions to respond to incidents involving external service providers that may directly or indirectly impact PROSEGUR GROUP 's activities, processes and assets.

The Supplier must have a supplier selection and evaluation process that assesses supply chain risks. Suppliers must be identified, evaluated and prioritized as part of the risk analysis and their treatment as other assets of the company.

The Supplier must at all times identify the subcontractors involved in the service to PROSEGUR GROUP and transfer the obligation to comply with the technological and security requirements described in this document.

The Supplier shall ensure that confidentiality agreements and service level agreements with minimum security requirements are identified when signing its procurement contracts with third parties, as well as other contracts that reflect the needs of the organization to protect the PROSEGUR GROUP's systems and data. These contracts should be reviewed periodically and compliance with them should be monitored.

The Supplier must ensure that both third party suppliers and users who have access to personal data and other information in the course of their work for the Prosegur Group undertake to store and treat such data with the utmost care and to the best of their knowledge and belief.

The Prosegur Group may request from the supplier information or reports on the measures and requirements taken with a particular supplier.

The supplier will be liable to the Prosegur Group for non-compliance with the requirements described in this Annex by the subcontractors involved in the service provided to the Prosegur Group, if this is the case.

The Supplier shall ensure that the provision of services by third parties is regularly monitored and audited to verify compliance with the established contractual agreements and, in particular, with the requirements set forth in this document.

In particular, the Supplier shall ensure the monitoring of changes to Supplier Services, taking into account the importance of the information, systems and business processes that fall within the scope of the third party's responsibility.

Failure to comply with any of the obligations contained in this Annex, both directly by the Supplier and indirectly by the companies contracted by the Supplier, may constitute grounds for termination of the Agreement or have other contractual consequences.

7.6. ANNEX V USE OF PROSEGUR IT RESOURCES AND SYSTEMS

Protective Measures

For the computer equipment supplied by PROSEGUR GROUP, the user must comply with the protective measures listed below:

The computer equipment must be used for professional purposes only.

The use of applications and web services based on audio or video streaming services, the purchase and sale of products, social media, news, sports and generally websites not related to professional activity is prohibited.

Users must store the information and files they process in the course of their work on cloud storage platforms shared and authorized by the organization (e.g., OneDrive) and avoid storing them locally on the device.

Users are responsible for ensuring that the devices assigned to them are not used by unauthorized third parties.

Sensitive information must not be shared with unauthorized third parties. Be especially careful with information transmitted by phone or over the Internet.

Users must allow the PROSEGUR GROUP authorized technical personnel access to their equipment in order to perform any necessary repair, installation or maintenance work.

Users must return the IT and/or the means of communication assigned to them by PROSEGUR GROUP when they terminate their activity in the organization.

If the IT or the means of communication provided by PROSEGUR GROUP are associated with the performance of a specific position or function, the person assigned to them must immediately return them to their IT entity when their relationship with said position or function ends.

The user must follow the indications and instructions to minimize the risks posed by malware threats. Special attention must be paid to the use of removable media, emails and software downloaded from the Internet or from unknown and/or illegal sources.

Systems found to be improperly used or not meeting minimum security requirements may be blocked or temporarily interrupted by PROSEGUR GROUP, with service restored as soon as the cause of the threat or degradation is eliminated.

The User shall not in any way violate the permissions of his account, in particular to install applications that are not related to his professional duties. If the User requires the installation of a specific application in order to perform his/her duties, he/she must submit a request to the Information Technology Department (hereinafter referred to as ITD) through the Service Portal.

It is not allowed to create personal accounts on the device for services that are not defined by the Prosegur Group.

It is expressly forbidden to access, download and/or store on any medium the following content: pages or illegal content that is inappropriate or contrary to morals and good customs; of image, sound or video formats; of viruses and malicious code; in general, of all types of programs and/or plug-ins without the express authorization of the Prosegur Group.

The user is responsible for ensuring that the devices assigned to him are up to date and have the appropriate security patches.

The Prosegur Group is authorized to monitor the activities on the computers to verify their proper use and to prevent and detect security incidents.

The use of removable media without prior authorization is prohibited.

USB ports are disabled by default. Should their use be required, a request must be made to the Information Security Department and the ITD, who must review the justification for such a request.

In case of approval, the user is responsible for the actions performed with the extracted information or information introduced into the Prosegur Group IT resources.

The storage media available are for professional use only.

The loss or theft of such media must be treated as a security incident and reported immediately.

The data carriers to be reused must first go through a secure deletion process according to the rules of the Prosegur Group.

Data carriers that are not to be reused must be destroyed by secure methods in accordance with Prosegur Group standards.

Return of equipment, devices and media

In the following situations:

• Completion of the service for which they are intended
• Termination of the user's contractual relationship with the Prosegur Group.
• Obsolescence of equipment, devices and/or media
• Breakdowns in equipment, devices and/or media

It must be returned by sending the device to the appropriate local microcomputer area through the designated channels with a request stating the reasons for the return:

In case of project cancelation: An unlisted service request must be opened in the service portal containing at least some of the following data:

o Serial number
o Hostname of the equipment
o Or the last user who used it: E.g. ES00605432.

Once a ticket has been opened, it is necessary to wait for the instructions provided by the local Microcomputer department regarding the return and collection of the equipment. In this case, the reuse

of the equipment by the user leaving the company to deliver it to the new company must also be confirmed by the ITD for security reasons.

In case of obsolescence or failure: Open a ticket in the service portal and follow the return instructions provided by the local microcomputing department.

In any case, the devices must NOT be left on the department's premises without physical and logical security controls, and they should not be used after being disconnected from the network for an extended period of time, as this jeopardizes the company's security due to possible vulnerabilities in the devices.

Clean desk and tidy workplace

Users are required to take the following measures:

• Keep the workplace clean and tidy so that there is no more material on the table than is required for the activity currently being performed.

• When a task or function is completed, the material must be moved to a secure area in an enclosed location. For this purpose, the Prosegur Group can assign lockable cabinets and drawers.

• Keep records and storage media containing confidential information locked away during extended absences and at the end of the day.

• Do not leave keys in the drawers or cabinets where confidential information is stored.

• Be careful with the information displayed on the screens of the device when you are around people who are not authorized to see this information.

• Working with information on paper should be avoided. Passwords and other important information should not be visible on paper or post-its.

• Make sure that documents for meetings, presentations and other events held in designated rooms are not left in those rooms after they are over.

• Always print with the "Secure Print" option enabled. A password must be entered for this.

• For all printers with password-protected printing mechanism, the employee must always make sure to log off.

• Immediately remove sensitive information from printers, copiers, and fax machines and ensure that no documents remain in the output tray or print queue.

• Destroy all discarded documents in a manner that prevents sensitive information from being read or easily retrieved. Use paper shredders or designated containers for this purpose.

• Cryptographic cards that could allow unauthorized persons to access Prosegur Group information and resources should not be left unattended and in plain sight.

Locking the workstation and sessions

The users of the systems have the duty to:

• Activate the screen saver and device lock when the workstation is left unattended.

• Lock the device while they are away Use devices that physically protect portable devices, such as padlocks, whenever available.

• Be sure to turn off equipment at the end of the workday.

• Images displayed after the screen is locked must not contain or reveal confidential information.

• If the workstation is left unattended during extended absences, applications and system sessions should be closed whenever their continued operation is not necessary for their functionality.

• Do not change the computer's auto-lock or auto-logoff settings without prior approval.

Access to information systems

Access authorizations

Users are responsible for keeping access authorizations, electronic identification and signature certificates, and software or other means assigned to them (e.g. cryptographic cards, tokens) for authorized access to Prosegur Group resources and systems.

Authenticators are unique to each person, non-transferable, and independent of the computer resource from which access is gained.

Use of Passwords

• Passwords must be difficult to guess.

• The following must not be used:
o Words from the dictionary, slang or dialect words.
o Words that refer to the context of the organization or the functions of the users.
o Words that contain personal information such as date of birth, names of
family members, people from a circle of confidence, phone numbers, etc.

• Users are responsible for keeping and using passwords.

• Passwords should be known only to the user who uses them. They should not be shared with third parties, even within the organization. All passwords should be treated as confidential information and used only by the assigned user. Passwords must not be shared over the phone, even if you are being addressed on behalf of the ITD or a supervisor.

• Passwords must not be transmitted by e-mail or other electronic means of communication.

• Passwords must not be written down or reproduced in any paper or document in which the password is recorded. They should also not be stored in text documents or notes on your computer or mobile devices.

• It is forbidden to use the passwords used for the accounts of Prosegur GROUP resources and services for accounts outside the company and vice versa.

• The user is obliged to change his passwords when the system informs him of the need to change them before they expire.

• The password should be changed immediately if there is any indication that it has been breached and reported in accordance with the established incident reporting process to the following email address: seguridad.informacion@prosegur.com

• Using mechanisms to remember passwords is prohibited. If you wish to use tools such as password managers, you must be approved and validated by Information Security and the ITD.

• The password should not be shared with anyone during vacation or extended absence.

• If the user needs to change the password and the system no longer allows it or the account has been locked, it must be reported as an incident to CAU through the Service Portal and an administrator will recover it by verifying the identity first.

Remote Access

VPN access allows users outside Prosegur Group facilities to access information and network resources by establishing an encrypted connection over the Internet.

In accordance with the foregoing, the following guidelines are established:

• The granting of remote access is based on the needs of the functions performed by individual users and may be revoked at any time if deemed appropriate.

• Remote access will be granted by the Prosegur Group in advance to those users who are assigned or who justify the need to work in this way.

• The use of remote access tools other than those approved by the Prosegur Group is prohibited.

• Users are responsible for protecting their remote access information, avoiding its disclosure and maintaining their privacy.

The user who uses remote access tools must ensure the physical security of the place where he/she uses the access, such as home, third party facilities, public places, etc.

• The user is solely responsible for the actions performed on the resources accessed during the VPN session.

• VPN access to the network and related resources is exclusively for professional purposes; any other use is considered unauthorized and the user bears full responsibility for it.

• Users with remote access who perform technical support, device management, or development tasks must not exceed their privileges.

• Employees and third parties authorized to use the remote connection shall have limited access for the development of their functions.

• It is prohibited to disclose or outsource to third parties the content of secret, confidential or internal information of the Prosegur Group accessed through the VPN service.

• Parallel connections are not allowed when connecting via remote access.

• In the remote access session, Internet access is possible only through the Prosegur Group proxy.

• Users are prohibited from connecting to public WI-FI networks to establish the Internet connection required for remote access. Although the information flow through the VPN is encrypted, this type of network does not have sufficient mechanisms to ensure confidentiality when browsing the Internet.

• The user must close remote VPN sessions when they are no longer needed for the function being performed or when he will be absent from his workplace.

• Prosegur Group can monitor access via a remote connection to prevent attacks and detect misuse.

Internet Access and Use

• Internet use is required for professional purposes only. Use for personal or recreational purposes is prohibited.

• Internet access is granted according to the requirements of the functions performed by each employee and may be withdrawn at any time if Prosegur GROUP deems it appropriate.

• Users undertake to use the Internet properly and are responsible for the sessions started on the Internet from any device.

• It is forbidden to store, transfer or outsource to third parties the content of information that is the property of the Prosegur Group, through any Internet medium accessible to the public or private, without the express consent of the company. The Prosegur Group may filter the content that can be accessed over the Internet. If a user justifies the need for access to a particular address, he must request it through his supervisor, so that he can request it from the IT department (hereinafter ITD).

• The Prosegur Group may monitor the activities of the users on the Internet and record the accesses.

• Unreliable sites or sites suspected of containing malicious content should not be visited.

• Under no circumstances is it allowed to change the configuration of the device's browsers (Internet options) or the activation of servers or ports without the permission of the ITD.

• It is expressly forbidden to download and/or store on a support pages with illegal, harmful, inappropriate or improper content, or content that is contrary to morals and good customs, and more generally any type of content that is contrary to the Prosegur Group Code of Ethics.

• Under no circumstances is the use and downloading of P2P files or similar allowed.

• Before using information from the Internet, you should check the extent to which it may be subject to intellectual or industrial property rights and/or violate applicable regulations on the protection of personal data.

• When exchanging information or conducting transactions, you should access websites by typing and checking the address in the address bar of the browser and not through external links. If the website is authenticated by a digital certificate, the user must verify its authenticity.

• The security of the connection must be verified by ensuring, among other things, that it is encrypted and that the HTTPS protocol is used for communication.

• The user must periodically delete the information stored in the browsers: cookies, history, passwords, etc. cookies, history, passwords…, etc.

• The installation of add-ons and plug-ins not previously approved by the Prosegur Group is prohibited.

• It is forbidden to use tools of any kind in the cloud that have not been previously approved by the Prosegur Group, for example to store or share information.

• It is forbidden to use the Internet access to participate in real-time discussions (chat/IRC channels), either through websites offering this service or through applications installed on the device (such as MS Messenger, TOM, Yahoo, ICQ or similar).

• The use of other means of Internet access (e.g. modems) that have not been authorized by the ITD area is not permitted.

• It is prohibited to use the Internet for purposes that may negatively affect the image of Prosegur GROUP, its representatives or third parties with whom it has a relationship.

Use of Email

Email is a tool provided by the Prosegur Group for the communication required by the development of its own activity with other companies or with other users. The following guidelines apply to the use of email:

• The access and use of these services by users, as well as the privileges associated with this access, must be limited to the rights established by their professional obligations.

• All email accounts that exist in the e-mail service are the property of the Prosegur Group.

• Users may only use the email tools and programs supplied, installed and configured by Prosegur Group.

• In the case of external personnel, the use of external addresses must be approved in advance by Prosegur Group.

• The email account is personal and non-transferable.

• Users are solely responsible for all activities carried out from their email accounts.

• Users are responsible for protecting their email credentials.

• The form and content of emails sent by the user must comply with the Prosegur Group Code of Conduct and under no circumstances may offensive, threatening or distasteful emails be sent.

• If it is necessary to send emails to multiple recipients, the “Bcc” field must be used to preserve the privacy of the
recipients' emails.

• The email box has a limited capacity. When the allocated quota is reached, the system informs the user about this situation. The user must then free up storage space by deleting the emails that are not necessary for the completion of his tasks.

• The user must empty the Recycle Bin on a daily basis, because the emails it contains are included in the quota allocated to each mailbox.

• The user must keep all mailboxes and folders sorted and classified. Unusable
emails should be permanently deleted.

• Attachments with a large byte size should be compressed before sending.

• The address bar should be checked before sending a message, and replies should be sent only to the correct person.

• Whenever possible, do not share documents via email, but provide a link to the resource.

• If you are sending critical or sensitive information, the message should be encrypted. When connecting over the Internet, log out at the end of the activity.

• Email is one of the main ways for malicious programs to enter computers and systems. Therefore, the following rules are established:

o Never click on mail links or open attachments unless the authenticity and reliability of the mail and its contents have been verified.
o Do not reply to unsolicited mails or mails of unknown origin, especially if they contain attachments. Such messages should be deleted immediately.
o Emails containing attachments with non-permitted extensions (.exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta) or with permitted extensions that obscure the non-permitted extensions should be deleted immediately. Emails containing such attachments should not be opened under any circumstances.
o It is prohibited to log in to services and websites with professional email accounts, except for authorized services.
o When forwarding or replying to an email, all irrelevant information such as addresses, signatures, headers, etc. must be deleted.
o Inbox preview must be disabled.

• All general email accounts and distribution lists have a responsible person who must adhere to the following rules:
o Use the inbox or distribution list only for the purpose for which it was set up (attention to customers, responding to inquiries, etc.).
o It is recommended to include a company signature when sending emails from this type of account.
o Responsibly authorize access and use of these accounts.

o Protect the reputation and image of Prosegur GROUP by maintaining a friendly tone in your responses.
o Check at least twice a year that the people who have been authorized are still valid.

• Any suspicious event should be reported to Corporate Information Security so that the necessary action can be taken. To facilitate this task, Prosegur Group has implemented a “Report Email” button in the mail applications.
• Prosegur Group may monitor the email accounts it makes available to its employees without prior notice to ensure the correct use and application of this resource and to detect possible security incidents.

Forbidden Applications

• Use of email for commercial purposes outside the company. Engaging in the distribution of “chain letters”, pyramid schemes, etc.

• Creating distribution lists without the ITD's consent.

• Massive dissemination of messages with inappropriate content that jeopardize the proper functioning of the Internet services.

• Sending or forwarding messages with defamatory, offensive or obscene content.

• Using mechanisms and systems that attempt to hide the identity of, or impersonate, the sender of the email.

• Sending SPAM emails of any kind (SPAM emails are those not related to work operations).

• It is not allowed to send attached files with .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta extensions, as these types of files enable the disguise of viruses and are usually used for their distribution.

• Spreading illegal content such as threats, malicious code, terrorism apologists, child pornography, illegal software or other criminal content.

Shared Storage

Shared storage resources are dedicated areas for storing and sharing documents and files developed as part of the professional activities of members of a work group.

All users who have access to shared storage resources must comply with the rules listed below:

• Users' access to and use of shared storage resources, as well as the rights associated with such access, must be limited to what is necessary for the performance of their duties (in compliance with the “need to know” principle).

• Under no circumstances may personal information be stored on shared storage resources.

• Storing executable or installable files (.exe) on shared storage resources without the control of ITD is prohibited.

• It is not allowed to request a shared storage resource for the exclusive use of one person.

• Backing up and restoring the information contained in shared storage resources is the exclusive responsibility of the ITD.

• All shared storage resources are assigned a responsible person to whom access authority to the shared storage resource is delegated. This responsible person shall review the access permissions to the shared storage resource at least every 6 months. The use of the allocated storage space in the storage resource is the responsibility of all authorized persons.

• In the event that historical information needs to be retained, the ITD may provide an alternative storage medium that ensures archiving of the information.

• For the storage of personal data in shared storage resources, the necessary technical measures and controls must be implemented to ensure compliance with the applicable legislation in this area.

Use of certificates and electronic signatures

• It is possible for the User to use certificates and electronic signatures as part of his activity in the Prosegur Group. The user must:
o Know and comply with the conditions for the use of certificates provided for in the Prosegur Group policies/rules and the restrictions on their use in accordance with the legislation in force.
o Handle with care the storage and preservation of signature or certificate data or other sensitive information such as keys, certificate request codes, passwords, etc., including the certificate media or the devices on which they are stored.
o Do NOT share the aforementioned data under any circumstances.
o Request revocation of the certificate in the event of suspected loss of confidentiality, disclosure, or unauthorized use of the data by notifying Information Security through the usual channels.

• In any case, the user is responsible for the use of such certificates and their safekeeping, otherwise this may lead to the activation of the corresponding sanction procedure.

Security Incident Management

If a user detects any type of anomaly or security incident that could jeopardize the security, proper use and/or operation of the computer resources or information systems to which he/she has access, as well as the information and personal data contained therein, he/she is obliged to immediately inform the Information Security Area so that the necessary measures can be taken, documenting the notification with the available evidence and documents.

• It must be notified through the following channels:
o By email to the Information Security department:
seguridad.informacion@prosegur.com

• The user is obliged to cooperate with the Prosegur Group in the investigation and rectification of the incident and, to this end, must hand over the affected computer resource, if necessary, or provide remote access to it, if necessary, so that the Prosegur Group's technical staff can carry out the appropriate checks and determine whether the resource can continue to be used safely.

USER STATEMENT ON THE USE OF PROSEGUR'S IT RESOURCES AND SYSTEMS

The user declares:

• It is the user's responsibility to protect and responsibly use the resources and tools assigned to him/her, always keeping in mind the established professional goals.

• The user is responsible for properly using the resources and equipment that are the property of the Prosegur Group, using them for the functions for which they have been assigned, respecting their integrity and using them only by the person assigned as responsible for them.

• It is the user's responsibility to read, understand and act in accordance with all other information security rules and documents, as well as any others provided by the Prosegur Group Management.

• That the User must inform the Corporate Information Security Area of any incident, anomaly or suspicion from an information security point of view that it considers relevant and that could affect the Prosegur Group.

• That the information stored on the devices and equipment is the property of the Prosegur Group and is subject to audit. The equipment must be returned to the Prosegur Group upon request at any time.

- When managing the resources of a Client, the User may also be subject to the security policy and rules approved by the Client in the performance of its tasks, if the Client so requests, without prejudice to the obligation to continue to comply with the provisions of the Prosegur Group.

- Failure to comply with the above rules and policies will result in the legal actions that the Prosegur Group may take to preserve its rights in accordance with applicable laws and agreements.

I DECLARE TO HAVE READ THIS DOCUMENT AND TO BE AWARE OF THE RULES FOR THE USE OF PROSEGUR'S IT RESOURCES SET FORTH HEREIN. _____, _____ of _____, _____

Name

Identity Document

Signed