



## **DATA ACCESS AGREEMENT**

[...], on [...] of [...], [...]

### **BY AND BETWEEN**

**On the one side**, Mr./Ms. [...], in the name and on behalf of the company [...], with N.I.F [...] and registered office in [...] (hereinafter, the “**Data Controller**”), in his capacity as [...] of the above-mentioned company, whose appointment and powers declares in force.

**On the other side**, Mr./Ms. [...], in the name and on behalf of the company [...], with N.I.F [...] and registered office in [...] (hereinafter, the “**Data Processor**”), in his capacity as [...] of the above-mentioned company, whose appointment and powers declares in force.

Hereinafter, individually each “**Party**”, and jointly the “**Parties**”.

Both Parties, recognizing sufficient legal capacity for the granting of this contract (hereinafter, the “**Agreement**”),

### **WHEREAS**

- I. Pursuant to the corresponding Agreement, the Data Processor has undertaken to provide the Data Controller with the services of [...] (hereinafter, the “**Services**”).
- II. The provision of the Services involves access by the CONTRACTOR COMPANY to personal data for which the CLIENT is **Controller** and **Processor / Controller / Processor**.
- III. For the execution of said Services, the Data Processor needs to treat the personal data held under the Data Controller’s responsibility.
- IV. In order regulate such access, both Parties agree to carry out this Agreement, which will be governed by the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 (hereinafter, the “**RGPD**”), by the implementing regulations thereof and, specially, by the following

### **CLAUSES**

#### **FIRST.- DEFINITIONS**

In this agreement, the following terms shall have the meanings, shall be binding, and shall contain and include everything defined hereinafter in accordance with Article 4 of the GDPR.

**PERSONAL DATA:** any information relating to an identified or identifiable natural person.

**PROCESSING:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring,



storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**FILING SYSTEM:** any structured set of personal data which are accessible according to specific criteria, whatever the form or modality of creation, storage, organisation and access.

**CONTROLLER:** a legal person that determines the purposes and means of the processing. For the purposes of this agreement, the CLIENT shall be deemed to be the CONTROLLER.

**PROCESSOR:** a natural or legal person that processes personal data on behalf of the CONTROLLER. For the purposes of this agreement, the CONTRACTOR and those companies that it needs to subcontract with for the provision of the engaged services shall be considered as the PROCESSOR.

## **SECOND.- PURPOSE.**

**2.1** The purpose of this Agreement is to define the conditions under which the Data Processor will carry out the processing of personal data needed for the correct provision of the Services rendered to the Data Controller.

**2.2** The rendering of the engaged Services involves the implementation by the CONTRACTOR of the following processing operations: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. **Note: add/delete processing operations as applicable.**

**2.3** In the event that the provision of Services involves the collection of personal data, the Data Processor will comply with the duty of information, according to the instructions provided by the Data Controller.

## **THIRD.- TERM.**

This Agreement shall be effective for the entire duration of the Services rendered to the Data Processor. Notwithstanding the foregoing, both Parties agree that the clauses of this Agreement, with express or implied intent to continue in force after the termination or expiration thereof, shall remain in force and continue binding both Parties as stipulated.

## **FOURTH.- PURPOSE OF THE PROCESSING.**

The personal data will be processed only to carry out the provision of the contracted Services. If the Data Processor considers necessary to carry out a processing of the data for a different purpose, he shall proceed to request the prior written authorization of the Data Controller. In the absence of such authorization, the Data Processor may not carry out such processing.

## **FIFTH.- NATURE OF DATA PROCESSED AND CATEGORIES OF DATA SUBJECTS.**

**5.1** The types of personal data that the Data Processor will process under this Agreement are the following **(those data that are not applicable shall be deleted, or added those applicable):**

- Identification data (name and surnames, NIF/ID Card, Social Security number/Mutuality, address, telephone, signature, footprint, image/voice, physical marks, electronic signature, other biometric data).
- Personal characteristics data (civil status, family data, date of birth, place of birth, age, sex, nationality, native language, physical or anthropometric characteristics).

- Social circumstances data (shelter/housing characteristics, ownerships or possessions, hobbies and lifestyle, membership of clubs or associations, licences, permits and authorizations).
- Academic and professional data (training/qualifications, student's records, professional experience, membership of colleges or professional associations).
- Details of employment data (profession, job position, non-economic payroll data, worker's history).
- Commercial information data (activities or businesses, commercial licenses, subscriptions to publications or media and literary, artistic, scientific or technical creations).
- Economic, financial and insurance data (incomes and revenues, investments and patrimonial assets, credits, loans and guarantees, bank data, pension and retirement plans, economic payroll data, tax deductions and taxes data, insurance, mortgages, subsidies and benefits, credit history, credit card).
- Transaction of goods and services data (goods and services supplied by the affected party, goods and services received by the affected party, financial transactions, remedies and indemnities).
- Behavioural data (consumption load curves, geolocation data or performance assessment data).
- Health or disability data.
- Data on trade union membership, religion, beliefs or relating to sexual life.
- Biometric data.
- Data relating to criminal offenses.

5.2 The stakeholders' groups whose data will be processed by the Data Processor under this Agreement are as follows (those that are not applicable shall be deleted, or added those applicable):

- Customers.
- Potential Customers.
- Supply point subscribers
- Suppliers.
- Contact people.
- Employees.
- Interns
- Contractor staff
- Temp agency staff
- Candidates in personal selection processes.
- Persons whose images are captured by video surveillance systems.
- Visits.

- Other

### 5.3. Criticality of the processor

To determine the security measures required of those listed in Annex I, and the monitoring mechanisms listed in Annex II for the purposes of this agreement, the CONTRACTOR is considered to be of **BASIC / MEDIUM / HIGH** criticality. (Note: delete as applicable according to the questionnaire to be provided by EDPR) and uses the **PROCESSOR's OWN SYSTEMS / EDPR's SYSTEMS** (Note: delete as applicable)

## SIXTH.- OBLIGATIONS OF THE DATA CONTROLLER

For the execution of the Service, the Data Controller undertakes the commitment to put at the disposal of the Data Processor the personal data and/or the information necessary for the appropriate processing of such data for the provision of the Services.

## SEVENTH.- OBLIGATIONS OF THE DATA PROCESSOR

7.1 The Data Processor undertakes to fulfil the following obligations:

- To treat the personal data only to carry out the provision of the contracted Services, in accordance with the instructions given in writing, at any time, by the Data Controller (unless there is a legal rule that requires complementary processing, in such case, the Data Processor will inform the Data Controller of that legal requirement prior to the processing, unless the Law prohibits it on public interest grounds).
- To maintain the duty of secrecy with respect to the personal data to which he has access, even after the termination of the contractual relationship, and to ensure that his dependants have committed in writing to maintain the confidentiality of the personal data processed.
- To ensure, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks of varying probability and severity for the rights and freedoms of natural persons, that he will apply adequate technical and organizational measures to ensure a level of security appropriate to the risk, including, where appropriate, among other things:
  - The pseudonymisation and encryption of personal data;
  - The ability of ensuring the confidentiality, integrity, availability and resilience continued of the systems and services treatment;
  - The ability of restoring the availability and access to personal data quickly in the event of a physical or technical incident;
  - A process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures in order to ensure the safety of the treatment.

When evaluating the adequacy of the security level, special account shall be taken of the risks presented by the data processing, in particular as a consequence of the destruction, loss or accidental or unlawful alteration of the personal data transmitted, stored or otherwise processed, or the communication or access not authorized to such data.

In the event that the implementation of specific and concrete security measures is needed, those measures will be added to this Agreement by means of an Annex.

- To keep under his control and custody the personal data to which he has access in relation with the provision of the Service, and to not disclose them, neither transfer or otherwise communicate

them, not even for their preservation, to persons unrelated with the provision of the Service covered by this Agreement.

However, the Data Controller may authorize, expressly and in writing, the Data Processor to use another data processor (hereinafter, the “**Subcontractor**”), whose identification data (full social name and N.I.F) and subcontracted services must be communicated to the Data Controller, prior to the provision of the service, at least with one (1) month in advance. The Data Processor will also inform the Data Controller of any change envisaged in the incorporation or substitution of the Subcontractors, giving thus to the Data Controller the opportunity to object such changes.

In case of making use of the power recognized in the previous paragraph, the Data Processor is obliged to transfer and communicate to the Subcontractor the whole obligations that for the Data Processor derive from this Agreement and, in particular, the provision of enough guarantees that he will apply appropriate technical and organizational measures, so that the processing complies with the applicable regulations.

In any case, access to the data made by natural persons who render their services to the Data Processor, acting within the organizational framework of the latter by virtue of a commercial and non-labour relationship, is authorized. In addition, access to the data is granted to companies and professionals that the Data Processor has hired in his internal organizational framework in order to provide general or maintenance services (computer services, consulting, audits, etc.), as long as such tasks have not been arranged by the Data Processor with the purpose of subcontracting with a third party all or part of the Services provided to the Data Controller.

- e. To delete or return to the Data Controller, at his choice, all personal data to which he has had access in order to provide the Service. Likewise, the Data Processor undertakes to delete the existing copies, unless there is a legal rule that requires the preservation of the personal data. However, the Data Processor may keep the data, duly blocked, regarding the responsibilities that could stem from his relation with Data Controller.
- f. To notify the Data Controller, without undue delay, of any personal data security breaches of which he is aware, giving support to the Data Controller in the notification to the Relevant Data Protection Agency or other competent Control Authority and, if applicable, to the interested parties of the security breaches that occur, as well as to provide support, when necessary, in the carrying-out of privacy impact assessments and in the prior consultation to the Relevant Data Protection Agency, where appropriate, as well as to assist the Data Controller so he can fulfil the obligation of responding the requests to exercise certain rights.

These notifications shall include at least the following information:

- Description of the nature of the security breach: categories and approximate number of data subjects concerned, and of records affected
- Identification of data protection officers
- Description of consequences
- Description of measures adopted or proposed by the CONTRACTOR to remedy the security breach

This information may be provided simultaneously or as and when it becomes available.

- g. To bring, in writing, a record of all categories of processing activities performed on behalf of the Data Controller.
- h. To cooperate with the Relevant Data Protection Agency or with other Control Authority, at its request, in the fulfilment of its power.



- i. To make available to the Data Controller the whole information necessary to demonstrate the fulfilment of the obligations established under this Agreement, as well as to allow and contribute to the performance of audits, including inspections, by the Data Controller or by a third party authorized by him. The lack of accreditation that the Data Processor is correctly complying with the obligations assumed in this Agreement, will be a cause of resolution of the same.

## **EIGHT.- LIABILITIES AND WARRANTIES**

**8.1** If the CONTRACTOR or any of its Subcontractors breaches this Contract or any of regulations when determining the purposes and means of processing, it shall be considered accountable for such processing, assuming all direct and indirect liabilities that may arise for EDPR as a result of such breach on the part of the processor.

**8.2** Likewise, both Parties agree that breach of these obligations shall be grounds for termination of the Agreement, so that breach by the CONTRACTOR, its employees or those involved in the provision of services on behalf of or at the request of the CONTRACTOR, shall empower the CLIENT to terminate the Agreement and shall give rise to the corresponding compensation for damages for breach of contractual obligations.

**8.3** Finally, and in addition to the foregoing, in the event of breach or defective performance of these obligations by the CONTRACTOR, and without prejudice to the possibility of termination of this Agreement by the CLIENT and compensation for any damages caused, the CONTRACTOR shall be obliged to pay the CLIENT, by way of a penalty clause, the amount equal to 2% of the value of the service contract to which this data processing agreement is linked.

## **NINTH.- PARTICIPANTS DATA**

The personal data included in this Agreement and those exchanged between the Parties to enable the provision of the Services will be treated by the other Party in order to allow the development, compliance and control of the agreed provision of Services, being the basis of the processing the fulfilment of the contractual relationship, keeping the data during all the time in which the said contractual relationship subsists and even later, until the eventual responsibilities derived from it prescribe. The Parties undertake to transfer to the owners of the data provided this information, as well as to inform them that they may write to the addresses indicated in the heading of this Agreement in order to exercise their rights of access, rectification, opposition and cancellation.

## **TENTH.- EXERCISE OF RIGHTS BY DATA SUBJECTS**

The CONTRACTOR shall pass on to the CLIENT any request to exercise the rights of access, rectification, erasure, objection, limitation and portability that it has received from data subjects whose data are processed as part of the provision of the service, so that it may be resolved by the CLIENT.

That notice must be immediate, in such a way as to allow the CLIENT to abide by the legally established deadlines for the exercise of rights by data subjects, and the CONTRACTOR shall be liable for any failure to comply with those deadlines due to failure or delay in notifying the CLIENT.

## **ELEVENTH.- CONSIDERATION**

The consideration for the services rendered is included in the terms and conditions entered into by the parties in the relevant service provision contract.

## **TWELFTH.- ENTIRE AGREEMENT**



This Agreement contains all the terms and conditions agreed to by the parties in relation to the subject matter hereof, and any representations, undertakings or promises, oral, written or implied, resulting from negotiations between the parties prior to this Agreement in relation to the subject matter hereof shall be deemed non-existent.

The fact that either party does not at any given time require compliance with any of the conditions set forth in this contract may not be construed by the other party as a waiver of any later demand for its performance.

#### **THIRTEENTH.- MODIFICATIONS**

Modifications to this agreement must be made by mutual agreement between the CONTRACTOR and the CLIENT. To this end, the party proposing the modification shall request the written consent of the other party at least fifteen (15) days prior to the effective date of the modification, and the other party shall give its response in writing within FIFTEEN (15) DAYS following receipt of the request. Failure to reply to the request for modification or to reply after the deadline for doing so shall be deemed to constitute non-acceptance of the request.

#### **FOURTEENTH.- EFFECTS OF TERMINATION**

Once the services have been provided, the CONTRACTOR and persons involved in any phase of the processing of the personal data shall destroy or return the personal data to the CLIENT, in accordance with the CLIENT's instructions, and any medium or documents containing any personal data subject to processing.

Destruction of the data shall not apply when there is a legal provision that requires retention, in which case the data must necessarily be returned to the CLIENT.

The data may only be retained by the CONTRACTOR for the period during which any liability may arise from the relationship established with the CLIENT under this agreement. In this case the data will be retained by the CONTRACTOR in duly blocked form, for which purpose it shall inform the CLIENT of the blocking system used.

In the event of termination, repudiation or rescission, regardless of the reasons for the termination, the CONTRACTOR shall cease to provide the services covered by this agreement immediately upon termination, and the confidentiality obligations established in this agreement shall survive indefinitely and remain in force, even after the termination of the business relationship between the parties for any reason whatsoever.

#### **FIFTEENTH.- NOTICES**

All notifications and communications that must be made under this agreement, such as notices, consents, authorisations, approvals and new instructions from the CLIENT, shall be made in writing, and shall initially be sent by fax, telegram, e-mail, registered mail or courier, to the addresses set out below.

CONTRACTOR / PROCESSOR:

- Mr/Ms XXXX
- Address: XXXX
- Telephone: XXXX Fax: XXXX



CLIENT / CONTROLLER:

- D./Dña. XXXXX
- Address: XXXX
- Telephone: XXXX Fax: XXXX

Either party may change such contact details by giving written notice to the other at least fifteen (15) days prior to the effective date of the change.

**SIXTEENTH.- NULLITY AND VOIDABILITY**

If any provision of this agreement is held to be void or voidable, in whole or in part, such nullity or voidability shall not affect the validity of any other provision of this agreement, which shall remain in full force and effect, unless the party claiming nullity or voidability proves that without the provision which is void or voidable the purposes of this agreement cannot be fulfilled.

**SEVENTEENTH.- APPLICABLE LAW AND JURISDICTION**

This Agreement shall be governed by the [INCLUDE APPLICABLE LAW ACCORDING TO THE GC CONDITIONS OF EDPR] and European regulations in terms of Personal Data Protection, as well as by the resolutions and guidelines of the Relevant Data Protection Agency and other competent bodies in this matter. In order to resolve any discrepancy regarding the interpretation and/or the enforcement of the provisions of this Agreement, both Parties submit to the jurisdiction of the Courts and Tribunals of [INCLUDE APPLICABLE LAW ACCORDING TO THE GC CONDITIONS OF EDPR] with express waiver of any other legislation or jurisdiction that may correspond.

And, in witness whereof, the Parties sign the present Agreement at the place and date indicated above.

**Data Controller**

**Data**

**Processor**

Fdo. [...]

Fdo. [...]

[...]

[...]

## ANNEX I

Criticality level of service provider	Contractually mandated security measures (clauses or documented additional instructions)	
<b>Basic</b>	Technical and organisational measures necessary under GDPR, specifically ensuring level of security adequate for risk (use of <b>standard clause, with no documented additional instructions</b> )	
<b>Medium</b>	<u>1. General security measures:</u>	
	<b>Use of Provider's Own Systems</b>	<b>Use of EDPR's Systems</b>
	<ul style="list-style-type: none"> <li>• Identification, dissemination and documentation of functions and obligations of personnel with access to data.</li> <li>• Maintain a written log of all categories of processing activities carried out on behalf of EDPR, pursuant to GDPR requirements.</li> <li>• Maintenance of internal log to ensure that people under their responsibility have committed in writing to uphold the confidential of the personal data processed, they know the rules and procedures to be adopted and are taking part in training in this field.</li> <li>• Design and implementation of user identification and authentication procedure.</li> <li>• Design and implementation of data access control procedure.</li> <li>• Design and implementation of incidence logging procedure.</li> <li>• Design and implementation of a backup copy procedure.</li> <li>• Implementation of procedure of inventory and control of incoming and outgoing media and documents.</li> <li>• Definition of criteria for archiving of media and devices for storage.</li> <li>• Design and implementation of periodic security controls to regularly test, evaluate and assess technical and organisational measures to ensure processing security.</li> <li>• Appointment of security manager(s) or of a Data Protection Officer.</li> <li>• Design and implementation of controls of physical access.</li> <li>• Design and implementation of service continuity plan.</li> <li>• Design and implementation of personal data pseudonymisation procedure where technically feasible.</li> </ul>	<ul style="list-style-type: none"> <li>• Identification, dissemination and documentation of functions and obligations of personnel with access to data.</li> <li>• Maintain a written log of all categories of processing activities carried out on behalf of EDPR, pursuant to GDPR requirements.</li> <li>• Maintenance of internal log to ensure that people under their responsibility have committed in writing to uphold the confidential of the personal data processed, they know the rules and procedures to be adopted and are taking part in training in this field.</li> <li>• Design and implementation of incidence logging procedure.</li> <li>• Implementation of procedure of inventory and control of incoming and outgoing media and documents.</li> <li>• Definition of criteria for archiving of media and devices for storage.</li> <li>• Appointment of security manager(s) or of a Data Protection Officer.</li> <li>• Design and implementation of controls of physical access, where appropriate.</li> <li>• Application of EDPR security policies and procedures</li> </ul>

<b>High</b>	<u><b>1. General security measures</b></u> (similar to those applied to managers with medium criticality level)	
	<u><b>2. Special security measures:</b></u>	
	<b>Use of Provider's Own Systems</b>	<b>Use of EDPR's Systems</b>
	<ul style="list-style-type: none"> <li>• Design and implementation of media encryption procedure</li> <li>• Design and implementation of an personal data anonymisation procedure where technically feasible</li> <li>• Design and implementation of a data access logging procedure.</li> <li>• Design and implementation of a communication encryption procedure.</li> <li>• Design and implementation of backup copy and recovery procedure.</li> <li>• Performance of regular independent audits (at least every 2 years) of compliance of legal requirements related to protection of personal data, including the GDPR / Independent certification of conformity with the GDPR (when certification mechanisms are available).</li> <li>• Adhesion to code of conduct on protection of personal data, pursuant to GDPR</li> <li>• Design and implementation of a procedure for secure and confidential destruction or return of data and documents (preventing any subsequent recovery and certifying non-existence of copies), when contractual relationship ends (except when obligation exists to preserve the data for an additional period, in which case the data/documents should be locked).</li> </ul>	<ul style="list-style-type: none"> <li>• Adhesion to code of conduct on protection of personal data, pursuant to GDPR</li> <li>• Design and implementation of a procedure for secure and confidential destruction or return of data and documents (preventing any subsequent recovery and certifying non-existence of copies), when contractual relationship ends (except when obligation exists to preserve the data for an additional period, in which case the data/documents should be locked).</li> </ul>

## ANNEX II

Criticality level of Service Provider	Contractually mandated supervisory mechanisms (clauses or documented additional instructions)
<b>Basic</b>	<p>The processor shall make available to EDPR all information necessary to demonstrate compliance with the obligations set out in the GDPR, as well as to allow and assist in the conduct of audits, including inspections, by EDPR or another auditor authorised by EDPR, and shall immediately inform EDPR if, in its opinion, an instruction contravenes the GDPR or other data protection provisions. <b>(standard clause)</b></p>
<b>Medium</b>	<p>The following specific mechanisms should be considered, in addition to those envisaged at the "low" criticality level:</p> <ul style="list-style-type: none"> <li>- Sending of log of processing activities performed on behalf of EDPR.</li> <li>- Sending of declaration on internal log that guarantees that persons under their responsibility have committed in writing to uphold the confidentiality of personal data processed, that they know the rules and procedures to be adopted and take part in training in this field.</li> <li>- Periodic sending of declaration/self-certification of compliance of with law and contractually-defined conditions on data protection;</li> <li>- Information and sending of supporting documentation to EDPR on any claim received from data subjects and the steps taken to resolve such claim;</li> <li>- Information and sending of supporting documentation to EDPR of any requests, queries or inspections undertaken by the supervisory authority with respect to data protection, the actions taken and the consequences thereof.</li> </ul>
<b>High</b>	<p>The following specific mechanisms should be considered, in addition to those envisaged at the "basic" and "medium" criticality level:</p> <ul style="list-style-type: none"> <li>- Sending to EDPR of a periodic independent audit report (at least every 2 years) on compliance of legal provisions related to personal data protection, including the GDPR;</li> <li>- Independent certification of conformity with GDPR (when certification mechanisms are available);</li> <li>- Adhesion to code of conduct on protection of personal data, pursuant to GDPR;</li> <li>- Periodic sending to EDPR of information on management compliance system of data protection obligations (governance model, identity of DPO, implemented policies and procedures, log of processing activities performed on behalf of EDPR, description of technical and organizational measures implemented, improvement action plans, etc.)</li> <li>- Sending of receipt certifying having informed your employees that their data is being shared with EDPR, when applicable, for relevant processing purposes (for example, management of access to EDPR systems, quality control, etc.);</li> <li>- Sending of certificate documenting secure and confidential destruction or return of data and documents (preventing any subsequent recovery and certifying non-existence of copies), when contractual relationship ends (except when obligation exists to preserve the data for an additional period, in which case the data/documents should be locked).</li> </ul>