

# Altamira MASTER AGREEMENT

Version 2020.1 – 25/08/2020

*This is a courtesy translation of the Italian version of this document. In case of ambiguity or disagreement between the two versions, the Italian document will be considered valid.*

## Chapter 1: Technical Support

### 1. Introduction

Altamira offers clients a technical support service to ensure maximum usability of the platform. This service is provided by telephone and e-mail. The service is available on Italian working days, from 09:00 to 18:00.

### 2. Definitions

**Reproducible bug:** an incorrect behavior of the platform that the client is able to reproduce; it is the Client's responsibility to reproduce the bug, i.e. the Client must tell Altamira which paths, clicks or actions generate the bug. Bugs have two levels of severity:

- **Critical Severity:** The Client is unable to perform an operation on the platform and it is not possible to identify a workaround. The functionality involved must be a key feature of the platform for the bug to be classified as critical.
- **Normal Severity:** The Client is unable to perform an operation on the platform but it is possible to identify a workaround. If a workaround cannot be found but the functionality is not a key feature of the platform, the bug is classified as normal.

**Non-reproducible bug:** an incorrect behavior of the platform that the client is not able to reproduce; the Client is not able to advise Altamira which paths, clicks or actions generate the bug. Examples of non-reproducible bugs include: sporadic reports by candidates who fail to complete submission of their CV, data lost in the platform, e mails not received by the recipient, etc.

**Workaround:** This is an alternative procedure that allows the Client to arrive at the same result they were trying to achieve when the bug occurred.

**Change request:** requests to change existing elements in the platform. For example, adding or removing fields, adding or removing lists, editing texts in the Career Center, changes in the PMP, etc.

**Reports:** Reports set up and accessible via the Reports section in the platform menu.

### 3. Standard Support

Standard Support includes:

- Explanations about how the platform works (provided that these explanations do not turn into a training course).
- Interventions on reports of reproducible bugs on the platform. Altamira undertakes to solve the problem by solving the detected bug or by indicating an alternative route allowing the client to perform the desired action (workaround).

Standard Support does not include:

- Change requests
- Report creation
- Resolution of non-reproducible bugs
- Restyling of the Career Center or development or modification of web pages
- Training

#### 4. Pay-per-use Client Service

In case the requested assistance is not included in the Standard Service, you can take advantage of the client service offered in a pay-per-use model. Pay-per-use client service can be made available in two ways:

- Per project. With this option, Altamira's technical consultants will conduct an estimate for the work to be carried out, which will be sent to the client by their sales representative. Once the offer is signed, Altamira will plan the activities according to the availability of its resources.
- By package. With this option, the client can purchase a number of days that can be used for customization or development activities, which they can allocate according to their needs. At the end of each month, Altamira will issue an invoice for the activities actually performed. The client can use the days package until the number of days purchased has been used up.

#### 5. Gold Support – No longer available

Gold Support allows the client to make small change requests on an ongoing basis.

Gold Support comprises Standard Support plus:

- Requests for changes to the set-up of the platform; such as, adding or removing fields, adding or removing lists, changes to the text in the Career Centre, changes to the PMP, etc.
- Setup of 3 additional customized reports per year

Gold Support does not include:

- Resolution of non-reproducible bugs
- Restyling of the Career Centre or webpage development or modification
- Training

The client undertakes to only use Gold Support in a fair and proportional manner. This means that Gold Support cannot be used to carry out tasks involving major modifications of the customer's configuration, or other tasks of long duration. A request for assistance covered by Gold Support should not require more than two working hours to fulfil. Requests for configuration changes or other tasks that would exceed two working hours must be billed as On-demand support.

#### 6. Support limitations

Altamira will make every reasonable effort to resolve any malfunction reported by the Client but does not guarantee that a solution will be found. In the event that the resolution of the problem requires an effort from

Altamira that is disproportionate to the problem caused by the malfunction, Altamira may opt not to solve the problem but rather suggest a workaround.

## 7. Security

As a matter of policy, Altamira does not manage users (for example creating new users, setting up user permissions, etc.). For security reasons Clients must carry out this activity themselves.

## 8. Summary table of the types of support

Summary outline of Support	Standard	Gold	On demand
Reproducible bugs	✓	✓	
Non-reproducible bugs			✓
Change request		✓	✓
Reports		2	✓

## 9. Guaranteed level of technical support service

Altamira undertakes to provide an initial response to tickets within 8 working hours of the ticket being opened and immediately give a first indication of the ticket's category. Based on the ticket's category, Altamira is committed to respecting the service levels shown below:

Type of support request	Resolution time from the opening of the ticket (working days)
Reproducible bug, high priority	3 days
Reproducible bug, normal priority	10 days
Requests for feature usage support	2 days
Change requests	10 days

## Chapter 2: Data centre, security, high availability, disaster recovery and privacy

### 1. Data centre - physical level

Altamira complies with current best practice in implementing physical level infrastructure in support of its own software platform, choosing to delegate the management and maintenance of its hardware devices to an IaaS (Infrastructure as a Service) provider. This solution, which is standard amongst many international companies, enables Altamira to focus on its core business of software development whilst attaining a higher service level than that offered by companies directly operating their own physical infrastructure.

In selecting its IaaS provider, Altamira guarantees that it:

- Is ISO 27001 certified
- uses appropriate firewall systems on its own network and on the network dedicated to Altamira
- uses suitable systems to detect intrusions and prevent Distributed Denial-of-Service (DDoS) on its own network and on the network dedicated to Altamira
- uses anti-malware systems
- uses cryptographic systems to protect data in transit between devices in the infrastructure
- uses only data centres with physical locations inside the European Union. In the event it becomes necessary to select data centres with physical locations outside the European Union (for example, for a disaster recovery site), Altamira guarantees that this data centre will be in full compliance with the privacy regulations applicable in the European Union.

### 2. Data centre - logical network

Altamira directly manages its own logical network with virtual servers created within the infrastructure of the IaaS provider. The infrastructure management is entrusted to a small group of long-serving Altamira employees who are granted the necessary authorizations to access the production environment on a personal basis. As concerns the logical layer, Altamira guarantees that:

- server and devices are regularly updated with patches released by their respective producers, with a minimum frequency of once per month;
- the servers are configured in line with best practices of the operating system or software producers by specialized staff with the requisite experience.

### 3. Security

Security is an integral part of the software development methodology, systems maintenance and customer support. To ensure the highest levels of security Altamira guarantees that:

- security is an integral part of the development process and the utmost priority is given to creating code which is secure and safe against common vulnerabilities such as SQL injection or Cross Site Scripting;
- employees have varying levels of access, depending on their role and their seniority and we use unique access credentials for information systems;
- access to the production environment is limited, both at network and authentication levels;
- all log-on operations to the system are recorded and stored;

- client data is always encrypted on the production disks, in the backup archives and in transit, using the appropriate protocols;
- suitable systems for intrusion detection and for the prevention of Distributed Denial-of-Service (DDoS) are in use on the network;
- anti-malware systems are used.

#### 4. High availability

Altamira's high availability is guaranteed both by the IaaS provider and by the way in which the services are constructed over the IaaS layer. Altamira is in a position to carry out normal cycles of system maintenance without any service interruption because the key services are structured so as to ensure high availability. For maximum service availability, Altamira guarantees that:

- the IaaS provider adopts all necessary measures to ensure high availability, such as geographic replication of data in different data centers, use of high availability technologies to accommodate all physical components;
- front end servers are redundant and accessible through load balancing;
- database servers are redundant both as regards applications and archiving;
- all other servers are redundant (DNS, contents, Active Directory, etc.) or if not redundant, their failure does not impact service availability.

#### 5. Disaster recovery

To offer the best possible service level, Altamira guarantees the implementation of a Disaster Recovery (DR) process using a different IaaS provider in combination with an on-premises architecture. The DR procedure will involve:

- a copy of all databases being maintained on a different IaaS provider or on the on-premises architecture;
- updating of the DR data copy at least every 8 hours with an hourly update under normal conditions;
- capability of the DR site to reactivate normal service in the event of catastrophic failure of the primary site, with such reactivation procedure being documented and regularly tested.

#### 6. Backup

The backup strategy is an integral part of the platform architecture's system administration process. Data is transferred to backup media as follows:

- data present in the database: every hour
- data present in the file system: every twelve hours

Backups are regularly restored to ensure they remain valid. Backup supports are encrypted.

#### 7. Privacy Policy

In addition to the guarantees required under the legislative decrees on privacy and European directives, as mentioned under "Terms and Conditions for the use of Altamira Services", Altamira undergoes periodic privacy audits. This task is undertaken by accredited law firms employing lawyers specialized in personal data protection.

## Chapter 3: Service levels

### 1. Service availability

Altamira commits to achieving or exceeding the following service availability levels:

Service Type	Minimum availability level	Normal availability level
Back office and other services available via web (e.g. career site)	99.7%	99.98%
Data transfer services (SFTP, FTPS)	99%	99.9%
Email dispatch services (SMTP)	99%	99.9%
Miscellaneous asynchronous services	99%	99.9%

### 2. Scheduled maintenance

Altamira may carry out scheduled maintenance at the following times:

- On public holidays: from 08:00 to 12:00
- 2nd and 4th Friday of every month: from 18:00 to 24:00

During scheduled maintenance periods services may be unavailable; this lack of availability will not count towards the service availability level.

### 3. Claims

Only for the Back office and other online services, in the event Altamira does not achieve or maintain the agreed Service Levels, the Client may be eligible to receive a Service Credit for part of the fees paid for the service.

For Altamira to consider a claim, the Client must submit a claim request to Altamira technical support desk, containing all the information necessary for Altamira to check it. The claim should therefore include, for example, a detailed description of the event, information about the time and the number of minutes of inactivity, the number and the locations of the users involved, (if applicable).

Altamira will review all the available information and determine, in good faith, within forty five (45) days, whether the Client is entitled to a Service Credit. Service Credits are issued as an amount to be deducted from the next invoice. To receive a Service Credit, the Client must have complied with the Terms and Conditions for use of Altamira Services. In the event that Altamira decides that a Client is due a Service Credit, the credit will be deducted from the next invoice issued for services provided.

The amount of the Service Credit will be calculated on a monthly basis, after first calculating the monthly service availability time using the following formula:

$$\% \text{ of availability time in the month} = (44640 - \text{duration in minutes of inactive time}) / 44640$$

and then applying the following table to calculate the Service Credit.

% of activity time in the month	Service credit
<99.5%	10% of the monthly subscription
<99.0%	25% of the monthly subscription

If the Client has payment terms other than monthly payment, the Service Credit will be calculated by converting the annual, six-monthly or other subscription to its monthly equivalent.

When calculating the % of activity time in the month, periods of scheduled maintenance will be excluded.

## Chapter 4: Altamira Terms and Conditions of Use<sup>1</sup>

These terms and conditions regulate both free trial and the purchase of our services.

Your acceptance of these terms and conditions will be indicated by clicking an acceptance box or by signing a Business Proposal referring to these terms and conditions. If acting on behalf of a company or other legal entity, you declare that you have the power to bind such entity and its affiliates to these terms and conditions, in which case the terms "You" and "Yourself" will refer to that entity and its affiliates.

**WARNING.** You may not access our Services if you are our direct competitors, except with our prior written consent. Furthermore, you may not access the Services for the purpose of monitoring their availability, performance or functionality, or for any other purpose relating to competition or commercial comparison.

### 1. Definitions

**"Affiliate"** denotes any entity that, directly or indirectly, controls, is controlled by the subject entity, or is subject jointly with it to common control. "Control," for the purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting rights of the subject entity.

**"Agreement"** denotes Business Proposal and these terms and conditions.

**"Malicious Code"** denotes viruses, worms, time bombs, Trojan horses and other computer codes, files, scripts, agents or malicious or harmful programs.

**"Business Proposal"** refers to the document outlining the economic conditions for purchases referred to herein. The Business Proposal shall be considered an integral part of the present agreement.

**"Services Purchased"** denotes the Services purchased by you through a Business Proposal, as distinct from those provided as a free trial.

**"Services"** denotes the platform and the online web applications supplied by us through website <https://www.altamirahrm.com> and/or other websites as described in the User Guide, as activated by you in the context of a free trial or on the basis of a Business Proposal.

**"User Guide"** denotes the online user manual for our Services which can be accessed through <https://www.altamirahrm.com>.

**"Users"** denotes individuals authorized by you to use the Services, for whom the subscription to a Service has been acquired, and to whom you have supplied user codes and passwords.

**"We"** or **"Ours"** denotes Altamira S.r.l, Tax Code 12940250157, present address: Corso Magenta 56, 20123 Milan, Italy, Telephone: +39 02 48100463, email: sales@altamirahrm.com.

**"You"** or **"Yours"** denotes the company or other legal entity on whose behalf you sign the Agreement.

**"Your Data"** denotes all the data or electronic information inserted by you into the Services Purchased by you.

### 2. Subject

#### 2.1. Subject of the contract

The subject of the present agreement is the supply of Altamira's HRM human resources management platform through the Internet via SaaS (Software as a Service).

---

<sup>1</sup> These Terms and Conditions are standard and may not be modified.



## 2.2. Provision of services purchased

We will provide you with the services purchased as laid down in the present Agreement and in the Business Proposal for the duration of the subscription period indicated in the Business Proposal, provided that the conditions of payment specified in the Business Proposal are complied with. The purchases undertaken by you through the present agreement are not subject to the future inclusion of features or characteristics (commonly known as “wish list” features), even if these features or characteristics are described orally or in writing by us.

## 3. Use of services

### 3.1. Our Obligations

We undertake to: (i) provide you with technical support for Services Purchased as described under Technical Support, (ii) take all commercially viable steps to ensure the Services Purchased are available 24 hours per day, 7 days a week, as described under Service Levels, with the following exceptions: (a) in the event of schedule maintenance as described under Service Levels or, (b) any non-availability resulting from circumstances beyond our reasonable control, including, but not limited to, force majeure, act of government, flood, fire, earthquake, civil uprising, act of terrorism, strike or other employment dispute (unless this only involves our employees), or telephone/internet service failure or delay, and (iii) we will provide the Services Purchased exclusively in compliance with applicable laws and the governmental standards.

### 3.2. Your obligations

You will (i) be responsible for user compliance with the present Agreement and the User Guide, (ii) be exclusively responsible for the accuracy, quality, integrity and legality of your Data and the methods with which they have been acquired; (iii) do everything commercially viable to avoid non-authorized access to or use of the Services, and will communicate any such unauthorized access or use to us in a timely manner; (iv) use the Services solely in compliance with the User Guide and applicable laws and the governmental norms. You undertake (a) not to use the Services to record or transmit illicit, defamatory, or otherwise illegal or illegitimate material, and not to record or to transmit material in violation of the right to privacy of third parties, (b) not to use the Services to record or transmit Malignant Code, (c) not to interfere with or prejudice the integrity or performance of the Services or third party data contained therein, or (d) not to attempt unauthorized access to the Services or to its systems or networks.

### 3.3. Free trial

Upon request, we will provide you with one or more Services on a trial basis for a period of 30 days.

Any data entered by you into the Services, or any customization applied by you or for you during the trial period, shall be definitively deleted at the end of the trial period. It is understood that during the free trial period the services shall be provided exclusively for evaluation and that no use shall be made of these Services for actual commercial purposes.

### 3.4. Relations with third parties

It is understood that the Services are offered exclusively to you and the fees are determined on this basis and in accordance with the other details laid down in the Business Proposal. You engage (a) not to make the Services available to anyone other than the Users, and (b) not to sell, resell, rent, supply or lend the Services.

## 4. Fees and Payment for Services Purchased

### 4.1. Fees payable by the User

You undertake to pay all the fees indicated in the Business Proposal and the further payments due as described in the present agreement, in line with the rates in force at the time. Unless otherwise indicated in the present

agreement or in the Business Proposal, (i) the payments are displayed to you and payable in Euro unless otherwise stated, (ii) the payments are due on the basis of services purchased and not their actual use, and (iii) the level of services purchased (for instance, the number of CVs in the database) may not be reduced during the relative billing period indicated on the Business Proposal. The fees for services purchased are based on billing periods established in the Business Proposal, beginning at the date of signature; therefore, fees for services added during a billing period will be charged for that entire period and the remaining subscription periods, unless otherwise stated in the Business Proposal.

#### **4.2. Billing**

Billing for Services Purchased is as described in the Business Proposal. In the event the billing details are omitted in the Business Proposal, the following billing periods shall apply: (i) an invoice shall be issued for an initial period selected by you and, thereafter, on the first day of every subsequent billing period until the termination of the present Agreement, as per Art. 11 of the present Agreement. All the invoices are payable on demand.

#### **4.3. Payment**

You undertake to provide us with valid and up-to-date credit card details, or a valid payment order on our bank account or other form of payment as authorized by us. In the event you provide credit card details, you authorize us to charge for the costs of all the Services listed in the Business Proposal. These charges and the aforementioned payments shall be made in advance, either annually or otherwise based on the billing periods indicated in the Business Proposal.

#### **4.4. Suspension of the Service**

In the event of a delay in payment of 15 days or more, we will contact you by normal email at the address of your offices as provided by you when signing the agreement, advising that payment has not been received. If we do not receive the payment within 15 days of the email communication, we will send a digitally signed email to the address recorded for you at the Chamber of Commerce. If after 15 days from the digitally signed email we do not receive payment for any amounts due under the present Agreement, we shall be entitled, without prejudice to your obligations regarding payment or of our rights and entitlements, to suspend our Services to you in accordance with Art. 1460 of the Civil Code, until such amounts due shall have been paid in full.

### **5. Proprietary rights**

#### **5.1. Reservation of Rights**

Without prejudice to the rights expressly reserved as set forth in the present Agreement, we reserve all rights, ownership and interest in the Services, including (but not limited to) all intellectual property rights relating to the platform and the web applications provided by us. The present Agreement does not guarantee you any rights other than those expressly laid down herein.

#### **5.2. Protection of Intellectual Property Rights**

You undertake (i) not to allow third parties to use the Services other than as expressly laid down in the present agreement or in the Business Proposal, (ii) not to create any derived works based on the Services, (iii) not to copy or use for framing and mirroring any part of, or content from, the Services, except to copy or insert as a frame on your internal network or at all events for your internal working purposes, (iv) not to carry out reverse engineering on the Services, or (v) to use the Services to (a) construct a competing product or service, or (b) copy any of the Service's characteristics, functions or graphics.

### 5.3. Ownership of your data

In the context of our relationship, you retain exclusive ownership of all rights, title and interest relating to all your data.

### 5.4. Suggestions

We shall hold free, total, transferable licence with the option to irrevocably, permanently and non-exclusively sub-licence, to use or to incorporate in the Services, any suggestion, request for improvement, recommendation or other comment provided by you, including by Users, relating to the operation of the Services.

## 6. Confidentiality

### 6.1. Definition of Confidential Information

In the present agreement, “Confidential Information” denotes all the confidential information provided by one party (“Informing Party”) to the other party (“Receiving Party”), either orally or in writing, that they define as confidential or that can reasonably be considered confidential by the nature of the information and the circumstances of its provision. Your Confidential information will include your Data; our Confidential information will include the Services; and the confidential information of both parties will include the terms and conditions of the present Agreement and of the Business Proposal, as well as the business and marketing plans, the technological and technical information, the designs and plans of the products, and the commercial processes made available by these parties. However, the Confidential Information (with the exception of your Data) will not include information that (i) is or becomes generally known publicly without any obligation towards the Informing Party being violated, (ii) was already known to the Receiving Party before being provided by the Informing Party, without any obligation towards the Informing Party being violated, (iii) is received from third parties without any obligation towards the Informing Party being violated, or (iv) has been developed completely independently by the Receiving Party. In no event shall the fact that there is a contract between the parties be deemed Confidential Information; either party may freely make it known that the Parties have a commercial relationship.

### 6.2. Protection of Confidential Information

Unless written permission is given by the Informing Party, (i) the Receiving Party will exercise the same degree of care that it uses to protect the confidentiality of its own, similarly confidential information (but under no circumstances less than a reasonable degree of care) so as to avoid making public the Confidential Information of the Informing Party for purposes external to the present Agreement, and (ii) the Receiving Party will limit access to the Confidential Information of the Informing Party to such of its own employees, contractors and agents as require access for the purposes of the present Agreement and who have signed confidentiality agreements with the Receiving Party, including safeguards no less stringent than those laid down in the present agreement.

### 6.3. Data Protection

Pursuant to and for the purposes of Legislative Decree 196/2003 (hereinafter referred to as the “Privacy Code”), as amended by Legislative Decree 101/2018 and the EU Regulation 2016/679 (“GDPR”), you appoint us external data processors as laid down in Annex 5: Appointment as external Data Processor.

### 6.4. Mandatory Disclosure

The Party receiving Confidential information (Receiving Party) from the Party providing it (Informing Party) may divulge such information wherever so required under the law, on condition that the Receiving Party advises the Informing Party of the need for such mandatory disclosure (within the limits foreseen in law) and provides reasonable support, at the expense of the Informing Party, should the Informing Party wish to contest the divulcation of the information.

## 7. Guarantees

### 7.1. Our Guarantees

We guarantee that the services will generally operate as described in the User Guide. Except as provided in this agreement, we make no additional guarantee of any kind, express, implied, statutory or otherwise, including any warranty of fitness for a particular purpose, to the maximum extent foreseen by applicable law.

### 7.2. Your Guarantees

You guarantee that you are not our direct competitor and that you will not access the Services for the purpose of monitoring their availability, performance or functionality, or for any other purpose involving commercial competition or comparison.

## 8. Compensation claims

### 8.1. Indemnities

You undertake to indemnify us and hold us undamaged, at any time, including subsequent to the maturity, recess or resolution, for whichever cause, of the present Agreement, from any prejudicial consequence, responsibility, burden or expense deriving from your use of the Data and Services in a manner which is illicit and/or wrong and/or in not in compliance with the Agreement and/or in violation of the rights of third parties and/or in violation of the law, engaging moreover to send us timely communication of eventual questions and/or claims received from third parties.

## 9. Responsibility - Collaboration

### 9.1. Responsibility

We shall be responsible to you in the event of service failure and data loss, as well as for gross negligence or fraudulent behaviour. Except where mandatorily decreed otherwise by the law, our responsibility under the present Agreement shall not exceed the net amount paid by you for the Services in the 12 months preceding the event which gave rise to such responsibility. Such limited responsibility shall not apply in the event of fraud or gross negligence.

### 9.2. Reporting obligations

Regardless of paragraph 10.1 above, you undertake to notify to us in writing without delay (a) at the beginning of the free trial period of the applicable Service or (b) at the start date of any Service activated by you, where the cumulative amount of foreseeable damages deriving from or relative to the present Agreement for eventual failure to provide the Services as described in the present agreement, exceeds the net amount payable by you under the present agreement for the Services over a 12 month period.

### 9.3. Notification of Faults, Errors and Damages Arising

To enable us to correct failures and errors in the services and so limit any resulting damage, you undertake notify us in writing within fifteen days, through our digitally signed email account, altamira@pec.it, of any fault and error and to supply us with information about the type and amount of the foreseeable damage arising therefrom. You undertake to adopt all necessary measures to limit as far as possible any damage caused. Our only obligation will be to take steps to repair such faults and errors as far as possible as described in Annex 1. Technical Support.

## 10. Duration and Termination

### 10.1. Duration of the agreement and termination

The services purchased by you begin on the date the Business Proposal is signed and continue for the duration stated therein. Unless otherwise stated in the Business Proposal, all services will be automatically renewed for periods of one year unless either party gives the other notice of termination at least 30 days before the end of the period. The price during the renewal period will be the same as that applied during the previous period except where we have given you written notice of a price increase at least 30 days before the end of the previous period, in which case the increased price will be effective from the date of renewal onwards. The aforesaid price increase will not be greater than 25% of the price for the same Services in the immediately preceding period, unless the price in such preceding period was indicated in the related Business Proposal as a special offer or lump sum.

### 10.2. Withdrawal for just cause

Either party may withdraw from the present Agreement for just cause: (i) by giving 30 days written warning to the other party in the event of significant violation if such violation is still present upon maturity of such period, or (ii) if the other party is subject to bankruptcy or any other proceedings related to insolvency, receivership, liquidation or cession of assets to creditors.

### 10.3. Reimbursement or Payment in the event of Withdrawal

In the event of your withdrawal for just cause, we will reimburse you all monies already paid for the residual period of all subscriptions successive to the effective withdrawal date. In the event of our withdrawal for just cause, we may withhold all monies already paid. In no event shall withdrawal relieve you of your obligation to pay us any monies due to us for the period prior to the effective date of withdrawal.

### 10.4. Returning your Data

The platform makes your Data available for download at all times, directly online in self-service mode. The technical procedures for downloading are those provided by the platform, which allows the downloading of all your data stored on the platform as a whole, in the Microsoft Excel, CSV and XML formats. Under no circumstances may you require us to supply the data using any other mode, unless you have agreed to a custom business proposal to return your data in a format specified by you. It is your responsibility to carry out the download of your Data from the platform within the date of effective closure of the subscription. Following that date, we shall have no obligation to hold or supply your Data and, from that moment, except where prohibited by law, we will cancel all your Data present on our systems or, in any case, in our possession or under our control. In the event you desire an additional period for the download of your Data, you will be required to stipulate an appropriate extension of the Services Purchased.

## 11. Final Provisions

### 11.1. Applicable Law and Jurisdiction

The agreement will be implemented in compliance with Italian law and the parties agree to accept the exclusive competence of the Court of Milan.

### 11.2. Communication Methods

Except where expressly indicated in the present Agreement, all alerts, permissions and approvals arising from the present agreement shall be made in writing and dispatched to you through: (i) digitally signed email, (ii) registered letter, or (iii) email (email will not be sufficient for the alerts mentioned under Articles 9, 10 and 11). Alerts will be routed to you through the system administrator selected by you for the various Services, and for alerts related to billing, to the billing contact designated by you.

### 11.3. Relationship between the Parties

The Parties are independent contractors. The present Agreement does not give rise to a company, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

### 11.4. No Third Party Beneficiaries

There are no third party beneficiaries of the present Agreement.

### 11.5. Waiver and Cumulative Remedies

Any failure or delay by a Party in exercising any right or remedy under the present Agreement will not constitute a waiver of such right or remedy. Except as expressly provided in the present Agreement, the remedies provided for in the agreement are in addition to, and do not exclude, any other legal remedy, or equity, available to the party. The parties agree in considering that the remedies established in the present Agreement shall be held as additional to, and not as a replacement for, the remedies established in law. Possible delays in exercising the rights foreseen in the present Agreement will not be taken as acquiescence and/or renunciation of the exercise of such rights.

### 11.6. Conservation

If any single condition of the present Agreement is deemed contrary to the law by a court having jurisdiction, the condition shall be modified by the court and interpreted in such a way as to best realize the original purposes of the condition to the maximum extent permitted by law, and the remaining conditions of the present Agreement will continue to be effective.

### 11.7. Cession

We reserve the right to cede the present Agreement in its entirety (including the Business Proposal) to any associate or in the event of fusion, acquisition, company reorganization, or sale of all or nearly all our patrimony, provided that the capacity to fulfil the conditions of the present Agreement remains unaltered.

### 11.8. Entirety of the Agreement

The present Agreement, with all its annexes and enclosures and the Business Proposal, makes up the entire Agreement between the parties and shall prevail over all agreements, proposals or declarations, written or oral, preceding or contemporary, regarding its subject. No modification, amendment, or renunciation of any condition of the present Agreement shall be considered effective unless executed in writing and signed or accepted electronically by the party affected by such modification, amendment or renunciation. In any case, in the event of conflict or incompatibility between the conditions laid down in the text of the present Agreement and any attachment, enclosure or Business Proposal, the terms of such attachment, enclosure or Business Proposal shall prevail. Regardless of any declaration to the contrary contained therein, no term or condition laid down in your purchase order or other order documentation (except the Business Proposal) will be incorporated or form part of the present Agreement, and any such terms and conditions will be null. Regardless of any ruling to the contrary, we reserve the right to periodically modify the present terms and conditions. These amendments will enter into force only if you sign a new Business Proposal referring to the modified conditions.

## Chapter 5: Appointment of external Data Processor

### Given that:

- The client is data controller ("Data Controller") of personal data loaded into the Altamira HRM human resources management platform pursuant to and for the purposes of Italian Legislative Decree 196/2003 (hereinafter, "Privacy Decree"), as amended by Legislative Decree 101/2018 and the EU Regulation 2016/679 ("GDPR").
- The Data Controller has entered an Agreement with Altamira S.r.l. (hereinafter "Data Processor") for the supply of outsourcing services (hereinafter, the "Services") described below and in the agreement itself, which, though not materially annexed, forms an integral part of the present appointment (hereinafter the "Agreement").
- As part of the services mentioned, the Data Controller will carry out the personal data processing operations described in Annex A ("Personal Data"), more clearly detailed in Annex B;
- The use of the Services implies outsourcing the following data to the Data Processor on the basis of Altamira HRM platform modules used:

Altamira HRM Module	Data outsourced
Altamira Recruiting	Candidate CVs
Altamira Employees	Employee personal data Employee payroll data
Altamira Performance	Employee personal data Employee performance assessment data
Altamira Leave Management	Employee personal data Employee leave management data
Altamira Attendance	Employee personal data Employee attendance management data
Altamira Payroll	Employee personal data Employee payroll data
Altamira Learning	Employee personal data Employee learning management data
Altamira HR Analytics	Employee personal data Employee payroll data

- The above include issues covered by Legislative Decree no. 196 of 30 June 2003 (hereinafter, "Privacy Decree") and EU Regulation 679/2016 (hereinafter, "GDPR"), as amended by Legislative Decree 101/2018, and it is therefore necessary to regulate the relationship between the parties, establishing specific tasks and instructions for the appointed Data Processor.
- With the present appointment, the Data Controller authorizes the Data Processor to further delegate to other parties, a list of whom will be maintained at the address:



<https://www.altamirahrm.com/en/trust/compliance/list-of-external-data-processors-for-altamira>. Any changes to the list of sub-processors will be announced with 45 days' notice through Electronic Certified Mail. In the event that the client objects to the appointment of any new sub-processor, the client may terminate the contract within 15 days of receiving the notice in the ways specified in Chapter 4, Article 10, thus halting the data processing on the part of Altamira. Altamira guarantees that, in case the contract is terminated due to opposition to the appointment of a particular sub-processor, the data belonging to the contracting party will not be transferred to that sub-processor, and that, in the absence of specific legal obligations requiring its preservation, this data will be erased irreversibly.

## All that being said,

with the present deed, the Data Controller, as described above and legally represented by the person signing this deed, in accordance with Art. 28 of the GDPR, and in consideration of their experience, ability and reliability,

## Appoints

Altamira S.r.l., with registered office in Via G. Marradi, 1, 20123 Milan, in the person of Its legal representative, as the external Data Processor for the Personal Data to which they has access during the provision of the Services herein referred to.

The Data Processor shall, specifically:

- carry out only those processing operations listed in Annex B required for the provision of the Services - including through use of their own appointed personnel (e.g. IT staff, Customer Service Engineers) and/or internal data processors and/or sub-contractors and/or system administrators, all duly appointed. All data processing operations necessary to the provision of the Services shall be carried out in full compliance with applicable laws and the general instructions contained in the present agreement and any subsequent agreements that may be communicated by the Data Controller, with explicit prohibition to make use of the data for scopes and purposes that are different than those indicated above;
- undertake any updating, modification, rectification and cancellation of Data as may be required for the purposes of the processing or upon request by the Data Controller;
- ensure the storage of the Data as laid down in Art. 5 of the GDPR and, generally, in compliance with the timeframes and modes expected under applicable law, even national;
- identify and adopt the security measures expected by the applicable Privacy Decree and, specifically:
  - a) minimize the risk of destruction, loss, even accidental, unauthorized access, and processing that is not permitted or not in accordance with the purposes of the processing of the Data, adopting, wherever this is within their area of responsibility and activity, the appropriate security measures, in accordance with the GDPR and the amended Privacy Code, and, in particular, by way of example and where applicable to the specific case involved: (i) to adopt a system of digital authentication with credentials of at least 8 characters, allowing access exclusively to appointed personnel and/or system managers and/or appropriate internal data processors in possession of authentication credentials; (ii) to adopt credential authentication management procedures, including their deactivation where left unused for at least 6 months or in the event of loss of eligibility to access the Data; (iii) to give instructions for regulating Data availability modes in the event of extended absence or unavailability of the appointed personnel that makes immediate action essential for operational and security reasons; (iv) to operate an authorization system for users and internal processors and system managers and to periodically update the processing rights of these persons; (v) to create and regularly update a list of appointed personnel; to protect electronic tools and Data against illicit processing and unauthorized access, adopting antivirus and other software aimed at avoiding electronic vulnerability, to be updated at least every six months; (vii) to adopt procedures for storing back-up copies, for restoring Data and systems, that envisage saving Data with a minimum frequency of at least once per week;



- b) to instruct their own appointed personnel and system administrators to ensure confidentiality of all third party personal data made known to them in the course of the Services, and likewise for processing, ensuring that credentials are never left unguarded or terminals left unlocked during a processing session;
- c) to adopt and respect, including respect by their own appointed personnel, internal data processors and system administrators, adequate technical and organizational security measures, in accordance with Art. 32 of the European GDPR, including by way of example and where applicable to the specific case involved: (i) measures and procedures aimed at ensuring system confidentiality, integrity, availability and resilience as well as availability and accessibility of Data in the event of physical or technical incident; (ii) procedures for ensuing notification of data breaches to the competent authority; (iii) staff training; (iv) policy, processes and tools adopted by Altamira to ensure and increase conformity with the GDPR; (v) encryption and pseudonymization measures; (vi) processes to test, verify and evaluate the effectiveness of the measures adopted; (viii) ensuring that their systems are set up in accordance with the principles of privacy by design and by default and that these include Impact Analysis of data protection and risk assessment on their own privacy procedures; (viii) storing records of processing undertaken and ensuring availability of such records to the Owner upon request; (ix) appointment of a Data Protection officer where necessary; (x) review of their own strategy of cross-border, online data transfer in accordance with the GDPR;
- to ensure that the appointed personnel, internal managers, external contractors, sub-contractors and system administrators, process the Data in full compliance with the Italian Privacy Decree and the European GDPR and, in particular: (i) that the processing is carried out in a lawful and correct manner, exclusively for the purpose of the performance of the Services; (ii) that the Data is processed only for the inherent purposes of the tasks assigned; (iii) that the data are not communicated or divulged without the prior authorization of the Data Controller; (iv) that they verify, in the event of any interruption, even temporary, of the processing, that the Data processed are not accessible to unauthorized third parties; (v) that they safeguard authentication credentials and keep them strictly confidential; (vi) that they comply with all security measures adopted by the Data Controller;
- to identify system administrators, where necessary, and appoint them in writing, fulfilling all the requirements laid down in the Provision issued by the Data Protection Authority on 27 November 2008;
- periodically, and at least annually, verify the conditions continue to exist for the storage of authorization profiles for appointed personnel, internal data processors and system administrators;
- to cooperate with the Data Controller in responding to requests from the Data Protection Authority, in the event of inspections and assessments carried out by the Authority;
- to ensure compliance with the instructions of the competent Data Protection Authority, informing the Data Controller about the processing of any requests from the Data Protection Authority or from any other judicial or public body, as well as of any relevant issue in the field of Data processing which may arise during the performance of the Services;
- to inform the Data Controller in a timely manner of any requests received from interested parties concerning the exercise of the rights foreseen under Arts. 15-21 of the GDPR;
- Where requested by the Data Controller, to give notice of Art. 13 of the GDPR and/or to request consent as laid down in Art. 6 of the GDPR and/or to arrange the request for processing of sensitive data and for the transfer abroad of personal data, in any case not foreseen under the general authorization issued by the Data Protection Authority;
- to allow the Data Controller the right of audit as foreseen under Art. 28 of the GDPR: in this context, to make all necessary information, where circumstances should require it, available to the Data Controller demonstrating compliance with the obligations spelt out in the present Agreement.
- in the event of withdrawal or termination for any reason from the present appointment, to interrupt all processing of the Data and, on instruction from the Data Controller, to arrange the return of the Data to

the Data Controller and, thereafter, the deletion of same within a reasonable time and in any case no longer than 60 days from the request;

- to notify the Data Controller of the processing of any violations of personal data (“data breach” or “data loss”) of which the Data Processor becomes aware, without unjustified delay. In the event that a “data loss” requires an operation to restore the data, the Data Processor will advise the Data Controller of the date of the backup from which Data is restored so as to ensure the Data Controller is aware of the exact time range of the lost data.

The Data Controller will periodically monitor the regular observance of the instructions given herein to the Data Processor and will verify the continued validity of the requirements of experience, ability and reliability which led to the appointment of the Data Processor.

If the Data Controller intends to carry out this auditing activity, the Data Controller will send to the Data Processor, with at least 45 working days’ notice, a written communication having as its object: i) a list of questions aimed at identifying the object of the auditing, which must in any case be limited to the activity that the Data Processor carries out on behalf of the Data Controller within the scope of the Contract; ii) a list of documents that the Data Controller intends to audit.

Please note that: (i) the documentary audits by the Data Controller can only be carried out remotely, via the encrypted transmission by the Data Controller of all the required documentation; (ii) the site visits, if any, which must be agreed with the Processor, cannot last more than 2 working hours in order to limit the impacts and slowdowns that such auditing could cause on the daily business activities of the Data Processor. This is without prejudice to the possibility that the parties could agree that such audits should be conducted outside working hours.

The Data Processor undertakes to offer any support necessary for such auditing activities, responding to requests for information and clarifications and providing any documentation requested.

In no case will the Data Processor give access to its information systems to the Data Controller in authenticated mode or allow access to the private networks of its information systems. It is understood that the Data Controller is allowed to perform vulnerability assessment (VA) or penetration test (PT) activities on the public endpoints of the Data Processor or its infrastructure partners, under the following conditions:

- that the VA and PT activity is requested by the Data Controller and authorized by the Data Processor through a written request made to [privacy@altamirahrm.com](mailto:privacy@altamirahrm.com) containing the details of the activity to be carried out
- that the VA and PT activities do not in any way harm the service provided by Altamira. In case the Data Controller damages the infrastructure or reduces the service levels of the Processor, the Data Processor may prevent the Data Controller from accessing their public endpoints by technical means, without prejudice to the right to compensation for damages.

For more information on auditing and inspection activities, please refer to the *Policy for the proper management of inspections*.

The present appointment does not entail any additional payment to the Data Processor beyond that already agreed in Agreement.

The Data Controller reserves, wherever necessary, the right to integrate the instructions contained herein and to adapt them on a case by case basis, including in accordance with any changes in the standards relating to data processing: to this end, the List of Data Processed and the List of processing Operations shall be updated and integrated with any other Data which may be further entrusted to the external Data Processor.

The appointment of the external Data Processor shall be effective from the date of signature of the present agreement and shall remain valid until revoked or until the Agreement terminates or until the termination of the Services and/or all data processing activity relating to the Data mentioned above.

For any issue not covered in the present agreement shall be subject to the general conditions applicable in Italian of personal data processing legislation.



**John Martelli**

*Internal data processor*

## Annex A: List of Data Processed

Below is the list of data processed by Data Processor, it being understood that for some processes on the Altamira HRM platform, data is entered by external parties over whom the Data Controller and the Data Processor have no control. For example, an application submitted by a candidate may contain personal details not included in this list. In the event that external subjects enter personal data outside those listed and the Data Controller becomes aware of this, these will be deleted from the platform. In the event the Data Processor notices the presence of data outside those listed, they will promptly notify the Data Controller of this.

It is understood that the Data Controller may add to the list of data processed, inserting further categories of data that the Data Processor may process, through additional appointments where required.

<input checked="" type="checkbox"/> Identity data:	<input checked="" type="checkbox"/> Sensitive data:	<input type="checkbox"/> Judicial data:
<input checked="" type="checkbox"/> name	<input checked="" type="checkbox"/> data relating to ethnic or racial origin (photo)	<input type="checkbox"/> data relating to ongoing criminal proceedings
<input checked="" type="checkbox"/> surname	<input type="checkbox"/> data concerning political leanings	<input type="checkbox"/> data relating to criminal records
<input checked="" type="checkbox"/> email	<input type="checkbox"/> data concerning religious or philosophical convictions	<input type="checkbox"/> data relating to pending charges
<input checked="" type="checkbox"/> address	<input type="checkbox"/> data concerning trade-union affiliation	<input type="checkbox"/> data relating to judicial records
<input checked="" type="checkbox"/> date of birth	<input type="checkbox"/> biometric data	
<input checked="" type="checkbox"/> tax code	<input checked="" type="checkbox"/> health-related data (protected categories that indicate their medical condition on their CV)	
<input checked="" type="checkbox"/> place of birth	<input type="checkbox"/> data relating to sex life/sexual orientation	
<input checked="" type="checkbox"/> telephone		
<input checked="" type="checkbox"/> mobile number		
<input checked="" type="checkbox"/> banking details (only for Owners who use Altamira Employees/Altamira HR Analytics or Altamira Payroll)		
<input type="checkbox"/> credit rating details		
<input checked="" type="checkbox"/> IP address		
<input checked="" type="checkbox"/> photo		

The Data processed concern the topics below:

- ☒ Candidates
- ☒ Employees
- ☒ Collaborators (trainees, interns, project personnel, freelancers, apprentices)
- ☒ Web users
- ☐ Customers
- ☐ Potential clients
- ☐ Suppliers
- ☐ Potential suppliers

## Annex B: List of processing operations

- |  |  |  |
|--|--|--|
| <input checked="" type="checkbox"/> Gathering    | <input type="checkbox"/> Modification            | <input type="checkbox"/> Communication           |
| <input checked="" type="checkbox"/> Recording    | <input type="checkbox"/> Extraction              | <input checked="" type="checkbox"/> Limitation   |
| <input checked="" type="checkbox"/> Organization | <input checked="" type="checkbox"/> Consultation | <input checked="" type="checkbox"/> Cancellation |
| <input checked="" type="checkbox"/> Structuring  | <input type="checkbox"/> Use                     | <input checked="" type="checkbox"/> Destruction  |
| <input checked="" type="checkbox"/> Storing      | <input checked="" type="checkbox"/> Elaboration  | <input type="checkbox"/> Comparison of data      |

## Chapter 6: Statement on the processing of client data

Altamira S.r.l, with registered offices in Via G. Marradi, 1, 20123 Milan, with Tax Code, VAT No. and registration at the Milan Chamber of Commerce no. 12940250157, in its role as Data Controller of the data processing (hereinafter “Data Controller”), informs you, in accordance with Art. 13 of EU Regulation 679/2016 (“GDPR”) and Legislative Decree no. 196 of June 30, 2003 (hereinafter “Privacy Code”), as amended by Legislative Decree 101/2018, that your data will be processed using the following modes and for the following purposes:

### 1. Scope of data processed

The Data Controller processes personal data (specifically, name, surname, company, business type, financial situation, hereinafter “Data” or “personal data”) supplied by you at the time of purchasing the Data Controller's products or services or, in general, pertaining to the contractual relationship with the Data Controller.

### 2. Purpose of data processing

Your personal Data are processed, without your prior consent (Art. 6, points b) and c) of the GDPR), for the following Service-related purposes:

- management of pre-contractual and contractual relations;
- performance of the contract;
- dispatch of Service communications via email, newsletter;
- management of payments and receipts;
- accounting purposes and related obligations;
- compilation and drawing up of tax declarations and related obligations;
- fulfilment of obligations laid down under applicable laws, regulations and Community law.
- exercise of the Owner's rights in judicial proceedings and in the management of any disputes arising;
- prevention and repression of illicit actions.

### 3. Processing methods

The processing of your Data will be undertaken as described under Art. 4 of the European GDPR, specifically collection, recording, updating, organization, conservation, consultation, elaboration, modification, selection, extraction, cession, use, interlinking, blocking, cancellation and destruction of the data, using the following methods:

- Paper copy (files)
- Digitized (through online network, pc and mobile devices, Salesforce, Zendesk and Office 365)

### 4. Nature of data provision and consequences of refusal to reply

Providing the Controller with the required data for the purposes outlined above is mandatory. Without the data it will not be possible to establish or to execute the contractual relationship with the Data Controller.

## 5. Data access

Access to your Data for the purposes set forth above may be granted to:

- the Data Controller's employees and associates, in their capacity as appointed processing personnel and/or internal data processors and/or system administrators;
- Third parties (for example, suppliers, professionals, banks, partners) carrying out activities through outsourcing on behalf of the Data Controller, in their role as external officers responsible for processing.

## 6. Data sharing

The Data Controller may communicate your Data without your express consent (as per Art. 6, points b) and c) of the GDPR) to the following parties who shall process them in their role as independent processing owners, whenever this is required of them:

- Finance Ministry, Governmental Tax Agency and ministerial agencies;
- Local authorities (regional, provincial, municipal);
- Regional and provincial tax commissions;
- Third parties (e.g., partners and corporate clients), which process the data in the performance of activities relating to the purposes mentioned above.

If your data is transferred outside the EU it will be in full conformance of Italian Privacy Regulations and European GDPR.

## 7. Data retention

The Data Controller will process the Personal Data for the time necessary in order to satisfy the purposes mentioned above, and in any event for no longer than 10 years from the termination of the contractual relationship.

## 8. Data transfer

Your Data will not be transmitted or transferred to non-EU countries.

## 9. Rights of the interested party

As an interested party, the Data Controller informs you that, with the exception of cases when legal limitations apply, you have the right to:

- obtain confirmation of the existence or non-existence of your personal data, even if not yet recorded, and have such data be made available to you in an intelligible form;
- receive and, where applicable, obtain a copy of information regarding: a) the origin and type of the personal data; b) the logic involved, in case of processing using electronic tools; c) the purposes and modes of processing; d) identifying information of the data controller and managers; e) the subjects or categories of subjects to whom the personal data may be communicated or who may come into contact with it, particularly if these are recipients located in third countries or international organizations; f) when possible, the data retention period or the criteria used to determine that period; g) the existence of an automated decision-making process, and, if this is the case, the logic involved, its significance and the consequences envisaged for the person concerned; h) the existence of adequate safeguards in the event of the transfer of the data to a non-EU country or to an international organization;

- obtain, without undue delay, the updating and correction of inaccurate data or, if you so require, the completion of incomplete data;
- obtain the erasure, blocking or transformation into anonymous form, whenever possible, of data in the following cases: a) it was processed unlawfully; b) it is no longer required for the purposes for which it was collected or subsequently processed; c) in case of the withdrawal of the consent on which the processing is based, and if there is no other legal basis for it; d) in the event you have objected to the processing and there is no prevailing legitimate justification for its continuance; e) if required to comply with a legal obligation; f) in the case of data pertaining to minors. The Controller may refuse to erase the data only in the following cases: a) the exercise of the right to freedom of expression and information; b) compliance with a legal obligation, the performance of a task carried out in the public interest or the exercise of public powers; c) public health reasons; d) archiving in the public interest, for scientific or historical research, or for statistical purposes; e) the exercise of a right in connection with a legal claim;
- have limits applied to the processing in the following cases: a) a dispute concerning the accuracy of the personal data; b) illegal processing by the Controller to prevent erasure; c) exercise of a right in connection with a legal claim; d) pending the verification whether the Controller's legitimate grounds take precedence over those of the interested party;
- receive, in the event that the processing is being carried out by automatic means, without impediment and in a structured, commonly used and readable format, the personal data relating to you, in order to transfer it to another Controller or – if technically feasible – to obtain the direct transmission of the data from the Controller to another Controller;
- object, in whole or in part: a) on legitimate grounds connected to your particular situation, to the processing of the personal data regarding you; b) to the processing of your personal data for purposes of sending advertising or direct sales materials, or for carrying out market research or commercial communications, through automated calling systems not involving an operator, via e-mail and/or through traditional marketing channels via phone and/or mail;
- submit a complaint to the Data Protection Authority.

In the above cases, whenever necessary, the Controller will advise any third parties with whom your Personal Data has been shared regarding any exercise of rights by you, except in specific cases (i.e. when this proves impossible, or involves an effort that would be manifestly disproportionate to the right protected).

## 10. Exercise of rights

You may exercise these rights at any moment:

- by sending a registered letter with delivery confirmation to the Data Controller's address;
- by sending a digitally signed email to [altamira@pec.it](mailto:altamira@pec.it);
- by phoning 39 02 48 100 463.

## 11. Data Controller, Data Processor and appointed processing personnel

The Data Controller is: Altamira S.r.l., Via G. Marradi 1, 20123 Milan.

The internal data processor is: John Martelli

The up-to-date list of data processors and appointed processing personnel is kept at the headquarters of the Data Controller.