Personal Data Processing Agreement

Personal Data Processing Agreement

I. PREAMBLE

Whereas:

A. Applicable Data Protection Laws allow any Data Controller responsible for Processing Personal Data to appoint a natural or legal person, public administration or any other entity or association to act as Data Processor for the Processing of Personal Data on the Data Controller's behalf among entities that can suitably guarantee, by virtue of their experience, capabilities and reliability, compliance with the Applicable Data Protection Laws, including with regard to security matters.

B. The appointed Data Processor shall provide sufficient guarantees to implement appropriate technical and organisational measures aimed at ensuring the protection of Personal Data and of the Data Subjects' rights.

C. This Data Processing Agreement, in conjunction with its Annexes, (collectively "**DPA**") is entered into between the Client (hereinafter: "**Client**"), namely the natural person or legal entity which purchased the Service (as defined below) and the details of which are specified below, and "Agence des Médias Numériques" ("AMEN") a French company *société par actions simplifiée*, based 12 Rond-point des Champs-Elysées 75008 Paris and registered under the SIREN number 421527797; the Client and AMEN collectively are referred to as "**Parties**", and each one individually as "**Party**", enter into this DPA to reflect the Parties' agreement with regard to the Processing of the Client's Personal Data, in accordance with the requirements of Applicable Data Protection Laws.

D. AMEN provides to the Client the service/s ("**Service/s**") activated by the latter in accordance with the contractual conditions set forth in the Service Order/s and in the General Conditions of Service, collectively available at this link ("**MSA**") and, in order to provide the aforementioned Service under this DPA, AMEN may Process Personal Data on behalf of the Client.

E. More precisely, the purpose/purposes of the Processing of Client's Personal Data with reference to the Service is/are described in Annex 1.

F. The Client acknowledges that its use of the Service may be subject to the related Applicable Data Protection Laws of jurisdictions that impose certain requirements with respect to the Processing of any Personal Data.

G. The Parties have entered into this DPA in order to ensure that they comply with Applicable Data Protection Laws and establish safeguards and procedures for the lawful Processing of Personal Data. The Client confirms that the provisions laid down in the present DPA reflect the obligations that the Applicable Data Protection Laws require AMEN to comply with, concerning the Processing of Client's Personal Data for the provision of

the Service. Accordingly, AMEN undertakes to comply with the provisions set forth in the present DPA.

The above preamble forms an integral part of the DPA.

1. DEFINITIONS

Unless otherwise defined in this DPA, all capitalised terms used herein shall have the meaning given to them in the MSA. In the event of any conflict or inconsistency in terms of data protection safeguards between this DPA and the Master Service Agreement, this DPA will prevail.

"Adequacy Decision" refers to a legally-binding decision issued by the European Commission allowing the transfer of Personal Data from the European Economic Area to a third country which has been considered adequate in terms of data protection safeguards.

"Applicable Data Protection Laws" means in EU member countries, the Regulation and complementary data protection laws in EU member countries, including any guidance and/or codes of practice issued by the relevant Supervisory Authority within the EU; and/or in non-EU countries, any applicable data protection law relating to the safeguarding and lawful processing of Personal Data.

"**Client**": means the subject who has purchased the Service.

"**Client Personal Data**" means Personal Data, relating to Data Subjects, Processed in connection with the Service provided by AMEN to the Client.

"Data Controller" means in general the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"Data Exporter" has the meaning set forth in the Standard Contractual Clauses.

"Data Importer" has the meaning set forth in the Standard Contractual Clauses.

"Data Processor" means in general a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"Data Subject" has the meaning set forth in the Regulation.

"Data Subject's Rights" means the rights recognised to the Data Subject pursuant to the Applicable Data Protection Laws. To the extent the Regulation is applicable, "Data Subject's Rights" means, e.g., the right to request from the Data Controller access to and

rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability.

"**DPA**" means this Global Data Processing Agreement in conjunction with its Annexes 1, 2 and 3.

"EEA" means the European Economic Area.

"**EU**" means the European Union.

"**List of Sub-processors**" means the list available in Appendix 3 to this DPA.

"**MSA**" means the terms and conditions provided in the Order/s of Service and in the Terms of Service regarding the provision of the Service agreed between the Parties and available at the following link: the General Conditions of Service.

"Non-EEA Sub-processor" means any entity, acting as Data Processor (or Sub-processor) and Processing Client Personal Data, for the provision of the Service, in a country outside the EEA, where such entity is not subject to the Regulation pursuant to its article 3, paragraph 2.

"**Non-EEA Controller**" means any entity, acting as Data Controller, to which AMEN provides the Services and which is established in a country outside the EEA, where such entity is not subject to the Regulation pursuant to its article 3, paragraph 2.

"Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. To avoid doubts, "Personal Data" has the meaning as set forth in the Regulation and Applicable Data Protection Laws.

"Process" or "Processing" means 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.

"Regulation" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"**Service/s**" has the meaning set forth in letter D. of the Preamble.

"Services Involving Non-EEA Sub-processors" means services provided by Sub-processors located outside the European Union.

"Special Categories of Personal Data" means Personal Data that reveals: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, including data relating to criminal convictions and offences or related security measures.

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to third countries pursuant to the Regulation, as approved by the European Commission in Commission Implementing Decision (EU) 2021/914.

"**Sub-processor**" means an entity engaged by AMEN to assist it in (or who undertakes any) Processing of the Client Personal Data in fulfilment of AMEN's obligations pursuant to the DPA, as listed in the List of Sub-processors, which has been approved by the Client pursuant to Art. 5 of this DPA.

"**Supervisory Authority**" means any authority which have the competence of monitoring and enforcing the application of the Applicable Data Protection Laws with respect to the Processing of Client Personal Data concerning the provision of the Service.

2. DATA PROTECTION ROLES

2.1. The Parties agree that:

a) The Client is the Data Controller of the Client Personal Data, except if and when the Client acts as the Data Processor of the Client Personal Data on behalf of a third-party which acts as Data Controller or as Data Processor itself. The Client, or the relevant Data Controller, determines the purposes of the collection and processing of the Client Personal Data;
b) AMEN acts, in any case, as the Data Processor of the Client Personal Data for the provision of the Service; and
c) this DPA regulates the relationship between the Parties in terms of respective duties and obligations concerning the Processing of Client Personal Data by AMEN, acting as Data Processor, in the provision of the Service.

3. AMEN'S OBLIGATIONS

3.1. The Client or the relevant Data Controller determines the purposes of Processing Client Personal Data for the provision of the Service.

3.2. In relation to the provision of the Service, AMEN undertakes to adhere to the following obligations including those defined in Annexes 1 and 2 attached hereto:

a) AMEN Processes the Client Personal Data only as necessary to provide the Service, subject to the Client's written instructions in this DPA;
b) AMEN notifies the Client in case it considers a Client's written instruction to breach Applicable Data Protection Laws. In no case is AMEN under the obligation of performing a comprehensive legal examination with respect to a Client's written instruction;
c) AMEN as Data Processor notifies the Client without undue delay of any contact or communication it receives from a Supervisory Authority in relation to the Processing of Client Personal Data. In this regard, the Parties acknowledge and agree that the responsibility for replying to such requests rests on the Client and not on AMEN;
d) AMEN has implemented operational, technical and organizational measures, including as described in Annex 2 hereto, aimed at protecting the Client Personal Data. The Parties acknowledge and agree that AMEN is specifically allowed to implement adequate alternative measures or use alternative locations as long as the security level of the measures or of the locations is maintained or strengthened compared to the declared measures;
e) In case AMEN discloses Client Personal Data to its personnel directly and exclusively involved in the performance of the Service, AMEN ensures that such personnel: i) is committed to confidentiality or is under an appropriate statutory obligation of confidentiality and; ii) Process Client Personal Data under the instructions of AMEN in compliance with its obligations under this DPA.

4. CLIENT'S OBLIGATIONS

4.1. The Client acknowledges and agrees that in order for AMEN to provide the Service, the Client shall provide AMEN with the Client Personal Data. The Client undertakes to verify that the security measures listed in Annex 2 of this Contract are compatible with the types of Personal Data that the Client intends to entrust to AMEN.

4.2. The Client represents and warrants that:

a) it has an appropriate legal basis (e.g., Data Subject's consent, legitimate interests, authorisation from the relevant Supervisory Authority, etc.) to Process and disclose the Client Personal Data to AMEN as part of the provision of the Service; and,

b) the provisions laid down in the present DPA reflect the obligations that the Applicable Laws require AMEN to comply with, concerning the Processing of Client Personal Data for the provision of the Service.

5. CONSENT TO SUB-PROCESSING

5.1. The Client acknowledges, agrees and consents that, for the sole and exclusive purpose of delivering the Service and subject always to compliance with the terms of this DPA, Client Personal Data may be Processed by AMEN or its Sub-processors as described in the List of Sub-processors.

5.2. Pursuant to Art. 5.1., AMEN has a general authorisation to engage Sub-processors provided that AMEN:

a) provides the Client with prior information as to the identity of the Sub-processors as described in the List of Sub-processors and notify the Client of any update in the List of Sub-processors so that the Client may object to the engagement of such Sub-processors;
b) enters into agreements with the Sub-processors containing the same obligations concerning the Processing of Client Personal Data as set out in this DPA;
c) exercises appropriate due diligence in selecting the Sub-processors and remains responsible for Sub-processors' compliance with the obligations set forth in this DPA;
d) at the Client's request, AMEN provides the Client with reasonable information as to actions and measures AMEN and its Sub-processors have undertaken to practically comply with the provisions set forth in this DPA.

6. TRANSFER OF PERSONAL DATA

6.1. Where the Client purchases one or more Services Involving Non-EEA Sub-processors, pursuant to Art. 5.1 and 5.2 above AMEN may transfer Client Personal Data to one or more further Sub-Processors which are Non-EEA Sub-processors and who are considered Data Importers for the purpose of the Standard Contractual Clauses. In such case, where there are no Adequacy Decisions applicable to the Non-EEA Sub-processor, AMEN commits to enter into the Standard Contractual Clauses with the Non-EEA Sub-Processor, and that only the clauses of the Standard Contractual Clauses under MODULE THREE: Transfer processor to processor apply (to the exclusion of the other MODULES).

6.2. Nothing in this DPA shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

6.3. Upon request, the Client may require the opportunity to review the Standard Contractual Clauses. To the extent necessary to protect business secrets or other

confidential information, including Personal Data, AMEN may redact part of the text of the Standard Contractual Clauses prior to sharing a copy.

6.4. The Client acknowledges that it is Client's responsibility to comply with any additional applicable duties and obligations in order to make the transfer of Persona Data to AMEN and to the Non-EEA Sub-processors lawful pursuant to the Applicable Data Protection Laws.

6.5. To the extent that the Client is a Non-EEA Controller, AMEN and the Non-EEA Controller agree that the Standard Contractual Clauses are hereby accepted as incorporated into this DPA by reference, as regards any transfer of Client Personal Data from the Non-EEA Controller to AMEN in the context of the provision of the Services. In this case, the following specifications apply to the Standard Contractual Clauses:

(i) Clause 7 of the Standard Contractual Clauses is applicable;
(ii) Only the clauses of the Standard Contractual Clauses under MODULE FOUR: Transfer processor to controller apply (to the exclusion of the other MODULES).
(iii) Clauses 14 and 15 do not apply, considering that the Services do not entail the combination of the Client Personal Data received from the Non-EEA Controller with other Personal Data collected by AMEN in the EU.
(iv) Under Clause 17 of the Standard Contractual Clauses, the laws of France will apply.
(v) Under Clause 18 of the Standard Contractual Clauses, the commercial Court of Paris (France) will apply.
(vi) Only Annex 1 of this DPA will apply and it will be deemed as Annex I of the Standard Contractual Clauses.

7. Cooperation and Accountability Obligations

7.1. The Parties collaborate in good faith to ensure compliance with the provisions of the present DPA, including, but not limited to, assuring the correct and timely exercise of Data Subject's Rights, managing incidents in case of security/Personal Data Breach in order to mitigate its possible adverse effects.

7.2 The Parties collaborate in good faith to make available to each other and to Supervisory Authorities the information necessary to demonstrate compliance with Applicable Data Protection Laws.

8. Data Subject Rights

8.1. Taking into account the nature of the Processing, AMEN assists the Client by appropriate technical and organisational measures for the fulfilment of the Client's obligation to respond to requests for exercising the Data Subject's Rights.

8.2. AMEN will provide Client with reasonable co-operation and assistance and provide such information as may be reasonably required for the purpose of responding to Data Subjects or otherwise in order to enable the Client to comply with its duties under Applicable Data Protection Laws in relation to the Data Subject's Rights. The Client acknowledges and agrees that in the event such cooperation and assistance require significant resources on the part of AMEN, this effort will be chargeable upon prior notice to, and agreement with, the Client.

9. DATA RETURN AND DELETION

9.1. AMEN will at no cost to the Client, return or destroy Client Personal Data upon request of the Client and upon the expiration or earlier termination of this DPA subject to a written request of the Client with reasonable advance notice, unless mandatory applicable laws (including but not limited to Applicable Data Protection Laws or law enforcement authority) including but not limited to Supervisory Authority, prevent AMEN from doing so.

9.2. With respect to specific requests from the Client for a return of the Client Personal Data, such request will be met to the extent feasible, subject to commercially reasonable technical and organisational constraints, which are commensurate with the volume and categorisation and the amount of Personal Data Processed.

9.3. Client’s Personal Data returned following AMEN's standard internal procedure shall be returned at no cost to the Client, otherwise it will be returned at a reasonable cost for the Client.

9.4. In case the Client opts for the deletion of Client Personal Data and save Art. 9.5, AMEN provides a statement assuring such deletion.

9.5. AMEN may retain Client Personal Data which is stored in accordance with regular computer back-up operations in compliance with AMEN’s disaster recovery and business continuity protocols (see Art. 12), provided that AMEN shall not, and shall not allow its Sub-processors to, actively or intentionally Process such Client Personal Data for any purpose other than the performance of the Service.

10. TRANSMISSIONS

10.1. Personal Data transmitted by AMEN in connection with the Service through the Internet shall be reasonably encrypted. The Parties acknowledge, however, that the security of transmissions over the Internet cannot be guaranteed. AMEN will not be responsible for Client’s access to the Internet, for any interception or interruption of any communications through the Internet, or for changes to or losses of Personal Data through the Internet.

10.2. If any Personal Data Breach is suspected, AMEN may suspend the Client's use of the Service via the Internet immediately pending an investigation, provided that AMEN serves notice of any such suspension as soon as reasonably possible and takes all reasonable measures to promptly restore use of the Service via the Internet and cooperate with Client in order to continue the provision of the Service via other communication channels.

10.3. The Client shall take all adequate and reasonable actions necessary to maintain the confidentiality of Client's employees' names and passwords for the Services. The Client shall be responsible for the consequences of any misuse of the Service by any Client's employee.

11. Personal Data Breach

11.1 The Client acknowledge and agree that AMEN shall not be deemed responsible for Personal Data Breach not imputable to AMEN's negligence.

11.2 If AMEN becomes aware of a Personal Data Breach, it will:

a) take appropriate actions to contain and mitigate such Personal Data Breach, including notifying the Client, without undue delay, to enable the Client to expeditiously implement its response program. Notwithstanding the above, AMEN reserves the right to determine the measures it will take to comply with Applicable Data Protection Laws or to protect its rights and interests;

b) cooperate with the Client to investigate: the nature, the categories and approximate number of Data Subjects concerned, the categories and approximate number of Personal Data records concerned and the likely consequences of any such Personal Data Breach in a manner which is commensurate with its seriousness and its overall impact on the Client and the delivery of the Service under this DPA;

c) where Applicable Data Protection Laws require notification to relevant Supervisory Authorities and impacted Data Subjects of such a Personal Data Breach, and as it relates to the Client Personal Data, defer to and take instructions from Client, as Client has the sole right to determine the measures that it will take to comply with Applicable Data Protection Laws or remediate any risk, including without limitation:

   i. whether notice is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required Applicable Data Protection Laws, or in Client's discretion; and

   ii. the contents of such notice, whether any type of remediation may be offered to affected Client Data Subjects, and the nature and extent of any such remediation.

12. Disaster recovery and business continuity

12.1 AMEN maintains commercially reasonable disaster recovery and business continuity protocols, which differ between each Service provided, a copy of the summary of which

is available for review by the Client upon request. AMEN may amend such plan at any time, provided that it shall not reduce its disaster recovery ability to less than the disaster recovery ability in effect pursuant to such plan as in existence on the effective date.

13. MANDATE

13.1 With the signature of this DPA, including Annexes 1, 2 and 3, the Client explicitly mandates AMEN to carry out on behalf of the Client, the activities described in Art. 5 above.

13.2 With the signature of this DPA, AMEN accepts the mandate, which will be carried out without economic remuneration in that it is in connection the Service, and legally signifies that AMEN has read and understood the instructions assigned.

The Client	Agence des Médias Numériques
Name and surname / name of the company _____	
C.F. / P. IVA _____	VAT NUMBER _____
Date and Place _____	Date and Place, _____
(Signature) _____	(Signature) _____

ANNEX 1

1. DATA SUBJECTS

The Personal Data Processed, according to the specific Service activated, may concern the following categories of Data Subjects, not determinable in advance:

- Client and/or employees and collaborators of the Client;
- Providers of the Client;
- Users of the Client;
- Customers of the Client;
- Data Subjects whose Personal Data are Processed by the Client by using the Service/s provided by AMEN.

2. CATEGORIES OF PERSONAL DATA PROCESSED FOR EACH SERVICE

The Personal Data Processed for any Service which may be provided to the Client, not determinable in advance, pertain exclusively to Personal Data in the meaning set forth in Art. 4 (1) of the Regulation, **with the express exclusion of Personal Data relating to criminal convictions and offences and Special Categories of Personal Data**.

In particular, the following categories of Personal Data will be transferred/Processed:

- Data of contact (name and surname, e-mail address, postal address, phone number);
- Date of birth;
- Age;
- Gender;
- Other categories of Personal Data Processed by the Client by using the Service/s provided by AMEN.

3. SPECIAL CATEGORIES OF DATA

The Personal Data Processed **do not pertain to Personal Data relating to criminal convictions and offences and Special Categories of Personal Data**.

4. PURPOSES OF THE PROCESSING

Personal Data may be Processed only for the provision of the Service as described in the MSA.

5. NATURE OF THE PROCESSING

The nature of the Processing operations varies on the basis of the specific Service activated through the MSA.

6. FREQUENCY OF THE PROCESSING

The frequency of the Processing operations varies on the basis of the specific Service activated through the MSA.

7. DURATION OF THE PROCESSING

The Client Personal Data will be retained for as long as the Service remains active.

ANNEX 2

Description of the Technical and Organisational Security Measures

AMEN and/or the Sub-processors undertake to maintain no less than the technical and organisational measures described below.

1) ORGANIZATIONAL MEASURES

a. IT security policy
Security policies are shared with all staff, they are reviewed following incidents and are updated periodically.

A policy on the acceptable use of corporate assets and their safekeeping is available.

b. Security roles and responsibilities
Safety roles have been identified and formally assigned, and also always available in case of need or incidents.

The structure of these security roles is periodically reviewed.

Employees are informed that for IT security reasons they must contact designated personnel, for whom they have a reference contact.

c. Background check for interviews and new staff
Any information provided by the candidates is verified during the interview.

d. Company policies
There is a member of staff formally dedicated to verifying internal compliance with company policies and to periodically updating them.

e. Incident and/or data breach management
A SIEM has been implemented to detect and report anomalies.

Security incidents are managed through a formalized, periodically updated procedure.

An incident register has been drawn up, which contains information relating to the discovery, analysis, containment, mitigation and recovery from each security incident.

To this end, a template for drafting reports relating to security incidents is available. The template is compliant with Articles 33 and 34 of the GDPR and periodically updated, where necessary.

Staff know who to contact in an emergency.

To measure the effectiveness of a response to a security incident, cyber exercises are carried out and
documented.

f. Personnel changes
New employees are trained on company processes and policies, including through specific procedures aimed at helping them understand the aforementioned. The assignment and modification of a user's permissions are performed through domain groups.

Employees credentials and assets must be returned when the employment relationship ends or they no longer need them, through a specific procedure for the revocation of company credentials and assets, which is periodically reviewed.

A periodic check is carried out on the effective removal of these assets or credentials of users who are no longer active.

g. Stock take and monitoring of IT tools
There is an asset management policy, which is periodically reviewed.

The critical systems within the company scope have been identified.

Both virtual and physical machines are initialized with a basic (baseline) configuration, which is kept up-todate over time.

A policy on the acceptable use of electronic tools is in force. The policy contains a procedure for the correct assignment and return of company assets.
The actual stock of the returned assets is checked periodically.

h. Business Continuity
The continuity of the offered services - or in any case of company operations - is ensured by means of emergency plans for restoring company operations.

Basic redundancy has been implemented for connectivity, electricity, services and data; such redundancies in place are mapped and are periodically adapted.

The use of resources is monitored and projections of them are made in order to plan adequate scaling and to prevent bottlenecks.

i. Change management
Adequate company policies and procedures are in place to make changes to critical systems, so that they take place in a predictable and safe manner, and which are further based on the degree of criticality of the systems which they refer to.

The changes made are adequately documented and automated tools are used for managing RFCs.

Users are notified in case of significant changes in their User Experience.

j. Vulnerability Assessment and Penetration Testing

Software and systems are properly tested before being placed in the production environment, thanks to a formalized procedure and the use of tools for the automation of tests.

Both the installation/uninstallation of patches and rollbacks are carried out through specific procedures, which are periodically reviewed.

Data used on the test databases are periodically updated.

Automated scans are carried out using tools to search for vulnerabilities as well as periodic sessions of Vulnerability Assessment and Penetration Testing (VA/PT), according to a formally established schedule.

The VA/PT sessions generate documentation, which is analyzed and shared with all other corporate functions involved, in order to identify further similar vulnerabilities within the corporate systems and to proceed with their removal. Specific security training is carried out periodically.

The Single Points Of Contact (SPOC) with the manufacturers and system vendors have been identified.

k. Contracts with suppliers

Appropriate contracts have been signed with the main suppliers of software, hardware and related assistance, containing SLAs and security requirements.

A template is used to request security measures from suppliers, and the right to carry out audits on suppliers is maintained.

l. Risk management

Risk Assessment methodologies have been followed, and take into account the threats that have an impact on data protection.

In particular, a risk analysis procedure has been drawn up and is periodically updated.
The main risks and their possible mitigations have been analyzed: the identified mitigation actions have been implemented.

These Risk Assessment activities are periodically re-performed.

m. Compliance
Compliance with standards and regulations is monitored through specific procedures, which are periodically reviewed.

Audits and assessments are planned in advance and in agreement with the personnel involved, to minimize the impact on business processes.

n. Interoperability and portability
A process allows the Data Subject to request their data in an interoperable format, guaranteeing thus the right of portability.

o. Safety training
Employees are periodically provided with material relating to safety issues; in particular, in order to increase their security awareness, training plans have been prepared, with personalized content according to the roles covered by the staff, and they are periodically updated. Staff knowledge of safety is periodically tested.

In this regard, employees can undertake, through the company, certification activities on safety issues.

p. Authorization
Each person authorized to process data receives clearly defined authorization profiles. These profiles are defined according to the minimization principle, and it is possible to list the authorized persons assigned to a given resource.

q. Removable media
The use of removable media is regulated.

Removable media are destroyed before being disposed of or sanitized before being reassigned.

2) TECHNICAL MEASURES

The description of the technical security measures applied to the company scope follows.

These measures, unless otherwise specified, are to be considered applicable to all tools and applications within the company scope.

a. Support utilities security
In order to ensure operational continuity, the supply of fuel for ground power units and batteries for uninterruptible power supplies is guaranteed.

In this regard, procedures for the management of fuel and batteries have been drawn up and specific supply contracts have been stipulated.

These procedures and contracts are reviewed whenever deemed necessary.

b. Access control to networks and systems
Authentication is centrally managed, all users are individual and it is necessary to authenticate before processing any personal data.

The users are associated with one or more authorization profiles, which, in turn, are assigned according to the need to know (minimization) and least privilege principles.

The effectiveness of the access mechanisms is periodically reassessed.

The network is segmented and the machines are authenticated before allowing them access to the network.

c. Security of data at rest
Critical data and the systems within which it resides have been identified.

Personal data available in the company systems are classified according to the "common", "particular" and "judicial" categories, furthermore, for the various types of data, the times of retention have been defined.

Procedures are also provided for the secure deletion of data at rest.

All assets have been surveyed and classified.

The use of removable devices is regulated, they are subjected to security checks before use, and the data on removable storage media is encrypted.

There are specific procedures for the disposal of assets, in particular, the disposal of assets is planned in advance, in order to prevent loss of information or the slowdown of operations.

Staff are informed about the provisions on encryption and the reasons for it.

d. Interface security
All users have a unique ID.

All interfaces use secure communication algorithms and the protection mechanisms adopted for their security are periodically re-assessed.

e. Backup Security and Disaster Recovery
We have a system for restoring data and services following disasters.

Specifically, a set of policies on backups, their conservation and security have been drawn up.

In particular, the backup procedure includes an external replication site containing the geographical backup of all data and the Disaster Recovery option for certain services.

f. Access to the data processing center and offices
According to the law, precautions have been taken against fires (fire doors, fire extinguishers, smoke detectors, etc.), documenting the related emergency procedures (e.g. fire fighting).

Anti-theft and/or CCTV devices are in operation; the conditions of the data center (humidity, temperature, cooling system settings, noise levels, energy consumption, etc.) are constantly monitored and the operation and effectiveness of the environmental measures implemented are periodically checked.

A list of personnel authorized to access company structures has been drawn up.

Visitor access logs have been prepared, which are maintained and stored according to a pre-established retention time, to then be deleted or destroyed.

Visitors are authenticated before allowing them access to the data processing center and/or offices and are always escorted/accompanied within the company premises.

g. Integrity of networks and systems
The following has been implemented: antivirus, antispam, SIEM, firewall with IDS or IPS functionality.

The updating and management of the anti-virus software takes place centrally.
Employees cannot disable protective measures on their machine. Any deactivations due to organizational reasons are periodically checked.

Inputs on applications and interfaces are adequately sanitized.

All protective measures are periodically updated or replaced if necessary.

h. Monitoring and recording systems
Monitoring and logging tools are in place for systems identified as critical and for actions of end users on the platform, keeping details on who performed which action.

These tools automatically raise alerts, when appropriate and, with the exception of user actions, generate full and unalterable logs, whose integrity can be verified;

The set of machines to be logged and monitored is periodically updated.

The rules for generating alerts and the list of information to be monitored are periodically updated.

i. Security requirements (security by design) and guidelines on writing secure code
We use guidelines for writing secure code.

Systems Development Life Cycle (SDLC) management tools are used; the development, test and production environments are separate and, in particular, the transition to production takes place through formalized test procedures.

The results of the assessments are shared with the developers, in order to increase their knowledge and prevent the recurrence of known problems.

j. Authentication
Each person authorized to process data passes a robust authentication procedure before accessing the data processing itself: this requires an alphanumeric password with a length of at least 8 characters, containing uppercase, lowercase and special characters.

The authentication credentials are individual for each person authorized to process data. The password assigned to a person authorized to processing data is changed by them at the first use and, subsequently, every three months.

The credentials of a person authorized to process data are reported to a system administrator if the authorized person does not use them for at least four months.

Consistent with any change of job of the authorized person, their credentials are deactivated or the authorization profiles assigned to them are modified.

A trustee is authorized to access, for unrelenting reasons of business continuity, the data processed by an authorized person who is absent for a long time, provided that he or she observes the confidentiality of the password - if in use - of the latter and promptly informs the absent person of the occurred access.

k. Data and device safeguarding
Each person authorized to process data safeguards all the devices assigned to them against accidental damage or theft, as well as their data processing sessions and the confidentiality of their credentials.

l. Defence
Company hardware/software systems supported by their manufacturers are constantly kept up-to-date.
The company systems developed internally are consistent with the data protection by design guidelines.

State-of-the-art protection programs are used, such as: Antivirus on all workstations, perimeter firewall, active IDS/IPS modules, personal firewall.

m. Availability of data
All data is subject to daily geographic backup.

n. Protection of data
All personal data is transferred electronically only in encrypted form.

ANNEX 3

Sub-processors	Country of establishment	Processing activities
UBILIBET	Spain	Provision of OBP services to Amen's customers
AMEN NEDERLAND	Nederland	Domain management
AMENWORLD	Portugal	Domain management
NAMESCO Inc.	United Kingdom	Domain management
NAMESCO IRELAND Inc.	Ireland	Domain management
NETWORK SOLUTIONS	USA	Domain names website design hosting
ALNILAM	France	Telecommunication services
REGISTER S.p.A.	Italy	• Datacenter Management; • Customers' credit card management (unique billing platform); • Server service management; • E-mail, Hosting, Website and E-commerce service management (in the context of the Group infrastructure management); • Customer Care services to the customers, comprising management of assistance requests, credit card withdrawal, management of requests from competent authorities; • Customer Care support in accessing to traffic data for and internal auditing;

		• Occasional support relating to any upload, modification, entry and deletion of data (access to Personal Data is only occasional, for specific assistance purposes); • Invoices recharge, costs the Group General Manager and of Group Management, statistical analysis; • Administration and finance, civil and fiscal management of accounting, drafting of the financial report; • Coordination related to profit and loss, management of administrative support data; • Registration and management of domain names (Register manages the Group's technical platform for domain operations); • Anti-fraud, consisting in cross-referencing the information gathered on Amen FR's website by means of cookies, fingerprint and e-tag with the billing code.
NOMINALIA INTERNET S.L.	Spain	Domain management Customer care support
AWIN AG	Germany	Advertising services, generation of leads online
DUDA Inc	USA	Provision of a platform to host and deliver sites to the Amen's customers
BASEKIT	Royaume-Uni	Provision of website development services
ePages GmbH	Germany	Provisions of e-commerce website building
LOGICA CONSULTING	Italy	Website creation

SITELOCK	USA	Provision of a IT system for the evaluation of malware presence and attack detection
WEBKORNER	Italy	Technical assistance and hardware maintenance