Annex
Security Measures

1. Description of technical and organisational security measures

The Processor undertake to guarantee a level of security no lower than that provided for by the technical and organisational measures described below.

2. System Administrators

The Data Processor and Sub-Processors is committed to comply with the Decision issued by the Italian Data Protection Authority , dated 27 November 2008 (and its subsequent amendments) entitled "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator”

2.1 Designation

The Processor is committed to draw up a letter of individual designation for each system administrator, following the evaluation of the experience, capacity and reliability of the subjects, containing an analytical list of the areas of operation.

2.2 Review of the work of the System Directors

The Processor is committed to proceed, at least once a year, with a process of reviewing the work of the system administrators through the means that they deem appropriate.

2.3 List of System Administrators

The Processor is committed to produce, at the request of the Data Controller, a list of the personnel designated as system administrator containing the list of the functions assigned .

2.4 Logging

The Processor is committed to implement an operational intelligence software that produces access logs relating to the systems on which the system administrators operate, having characteristics of completeness and inalterability as well as being subject to integrity verification and to be kept for at least 6 months.

3. Authentication

3.1 Credentials

The Processor is committed to create an alphanumeric password consisting of at least 8 characters in length, containing upper/lower case letters and special characters. Alternatively, The Processor is committed to guarantee the possession of a token or, for processing of particular importance in terms of both legal and criticality for the core business of the Data Controller, the verification of univocal and univocally digitized biometric characteristics such as fingerprinting. The Data Processor and the Sub-Processors is committed to proceed, if necessary, at the express request of the Data Controller, with the combination of two or more authentication factors. The Processor is committed to apply this password policy to all company systems and applications.

3.2 Periodic modification

The Processor is committed to force an automated periodic password for its System Administrators, the change is set to be last less than 90 days. The Processor also undertake to technically force a password change at the first access for new System Administrators.

3.3 Individual Credentials

The Processor is committed to not assign shared credentials but is committed to assign only individual credentials, in particular with regard to figures with high permissions on systems and applications.

3.4 Reporting inactivity

The Processor is committed to ensure that all credentials of its System Administrators, except those used for technical management purposes only (e.g. machine users or root credentials), are reported as inactive after 6 months.

3.5 Deactivating or changing credentials

The Processor is committed to operate in order to guarantee that all credentials, except those used for technical management purposes only (e.g. machine users or root credentials), must expire automatically after six months at the latest or be updated in relation to the change of duties of the person in charge.

3.6 Non-disclosures

The Processor is committed to implement and document appropriate procedures for accessing the data in the event of the prolonged absence of the person in charge who holds them. These procedures should not, in any case, provide for the disclosure of the password of the person in charge.

4. Data and Device Protection

4.1 Protection of credentials

The Processor is committed to draw up a policy containing clear instructions on the precautions to be taken to ensure the secrecy of the credentials and the diligent custody of the devices assigned.

4.2 Protection from damage and theft

The Processor is committed to draw up a policy containing clear instructions on the precautions to be taken to ensure the protection of the devices assigned.

4.3 Session protection

The Processor is committed to implement a lock screen/screensaver system with the re-entry of credentials whenever there is not physically an employee present to supervise/use the workstation. This lock screen should be set so that it activates automatically after less than 20 minutes of inactivity.

5. Authorization

5.1 Authorisation profiles

The Processor is committed to implement a centralised system for the management of authentication and authorisation. The Processor is committed to proceed to a census of the authorization profiles, before assigning them.

5.2 Minimizing permissions

The Processor is committed to proceed in a residual way, not assigning more permissions than necessary and respecting the principles of least privilege and need to know, i.e. allowing the visualization only of the data necessary to carry out the work function, with the attribution of minimum permissions on systems and applications.

5.3 Profile review

The Processor is committed to verify the consistency of the authorisation profiles at least annually and proceed with the reporting of such activity.

6. Defence

6.1 Updates

The Processor is committed to monitor and manage the updates in a centralised and/or automated manner, or to adopt suitable organisational means in such a way as to make the machines and applications constantly updated, taking particular account of security updates.

6.2 Isolation of systems no longer supported

The Processor is committed to segregate the machines that for operational reasons are still in use even though they are no longer supported by updates.

6.3 Data protection by design

The Processor is committed to formalise or adopt data protection by design guidelines, ensuring that the company systems developed internally are consistent with them.

6.4 State of the art protection programmes

The Processor is committed to implement and maintain updated protection software such as antivirus, which should be managed preferably centrally, firewall, antibot, antispam.

7. Data availability

7.1 Backups

The Processor is committed to implement a backup system, formalising a backup plan, documenting the technologies in place within a policy that also contains a procedure for correctly carrying out this activity.

8. Data protection

8.1 Encryption in transit

The Processor is committed to implement and document the encryption technologies in transit.

9. Removable devices

9.1 Removable devices

The Processor is committed to regulate the use of removable media and their protection.

9.2 Sanitization of removable devices

The Processor is committed to formalise appropriate procedures for the destruction, encryption and/or formatting of removable devices and company devices in use.

10. Security roles

The Processor is committed to define the corporate function who is responsible for cybersecurity, i.e. who can cover it in the company with the relative responsibilities. This may involve appointing a CISO (Chief Information Security Officer) or, more generally, a CSO (Chief Security Officer) or, generally, a person who has the authority, in the company, to perimeter, under the security, information technology and information, the processes of the organization. This figure should be available to detect security incidents and should be known to all employees.

11. Third parties

11.1 Contracts

The Processor is committed to draw up all relevant contracts with outsourcers and suppliers in such a way that they also include the security requirements relevant to the service provided or product supplied.

12. Asset Management

The Processor is committed to remove assets and credentials of employees who are no longer in force within the infrastructure of The Processor, or who have changed the task and assets necessary to carry out the task.

The Processor is committed to carry out a periodic verification of the effective removal of assets and credentials.

13. Physical security of the Data Center

13.1 Physical security measures

The Processor is committed to set up physical security measures, such as, for example, the installation of burglar alarms and CCTV, both at the headquarters and at the entrances to the Data Center.

13.2 Visitors

The Processor is committed to authenticate visitors before accessing the Data Center. The Processor is committed to accompany visitors within the structure of the Data Center and to prepare an access register for them.

13.3 Conditions of the Data Center

The Processor is committed to constantly monitor the conditions of the Data Center, taking into account the variables relating, among others, to temperature, condition of the cooling system, dust, humidity and to periodically check the functioning of the sensors.

14. Access control

14.1 Individual credentials

The Processor is committed to commit themselves to set individual credentials for each person in charge and forbid them in sharing such credentials.

14.2 Authorisation profiles

The Processor is committed to undertake, within the limits of what is permitted by the systems, to create authorisation profiles to which the users created are assigned.

14.3 Network access control

The Processor is committed to evaluate the possible introduction of a solution for NAC (Network Access Control) in order to authenticate the machines on the network.

14.4 Rate limiting

The Processor is committed to set a maximum number of failed login attempts before blocking the account on all company systems and applications.

15. System Integrity

15.1 SQL Injection

The Processor is committed to commit to implementing input sanitization processes in order to avoid known attacks such as SQL Injection.

15.2 Absence of possible deactivation

The Processor is committed to undertake not to allow the persons who are not in charge of security functions, to be able to deactivate the protective measures on their machines.

16. Vulnerability assessment and penetration testing

16.1 Scheduling

The Processor is committed to conduct sessions of vulnerability assessment and penetration testing on the company's systems on a regular basis.

16.2 Penetration Test

A 360° penetration test has been conducted on the service and on all endpoints, infrastructure and portals associated with the API product.

17. Management of incidents and violations

17.1 Incident handling procedures

The Processor is committed to introduce practices, protocols and procedures relating to incident handling and manage all security events and/or security incidents through a formalised procedure with pre-established roles.

17.2 Staff training

The Processor is committed to inform the personnel regarding the incident handling procedures.

17.3 Alerts

The Processor is committed to consider, if deemed functional and appropriate to the risk, to adopt a SIEM, or alternative solutions that achieve the purpose of reporting anomalies and/or attacks in progress.

17.4 Record of incidents

The Processor is committed to draw up and maintain a record of incidents, containing at least information on discovery, analysis, containment, mitigation and recovery from the various security incidents.

17.5 Communication to the Data Controller

The Processor is committed to promptly notify the Data Controller, within 24 hours of having become aware of it, of any security incident that have occurred on their infrastructure.

18. Data Availability

18.1 Load Test

Transverse load tests have been implemented on several endpoints in order to verify the workload that will be able to support the infrastructure. The load of requests generated by the load tests is in line with the traffic volume expected to be received. The Service Level is guaranteed by the Sub-Processor.

19. Training

The Processor is committed to formalise periodic security awareness training for all office staff, in order to reduce the possibility of intrusions, successful phishing or malware infection.

20. Recording of operations

The Processor is committed to implement an operational intelligence software that produces unalterable logs, complete and subject to integrity verification that operates on the systems on which the personal data referring to the Data Controller are processed.

21. Software development and environment management

21.1 Development guidelines

The Processor is committed to implement and adopt guidelines for writing secure code.

21.2 Separation of environments

The Processor is committed to separate the test, development and production environments. The test, staging and production environments are only present in the cloud and are physically separated, i.e. each is hosted on an environment-specific physical node.

21.3 Formalization of production processes

The Processor is committed to formalise the procedures necessary for the transition from the test environment to the production environment.

21.4 Testing

The Processor is committed to test software and systems after they have been put into production.

21.5 Patches

The Processor is committed to install and uninstall the patches using known practices.

21.6 Protection of test data

The Processor is committed to protect the test data by obfuscation or encryption and to make them usable by authorised personnel.

22. Change management

22.1 Formalisation of change management

The Processor is committed to make changes to critical systems through known practices or formalised procedures.

22.2 Notification to the Data Controller

The Processor is committed to notify the Data Controller of any significant changes to the User Experience.